Canad. J. Math. Vol. **57** (5), 2005 pp. 1102–1120

Power Residues of Fourier Coefficients of Modular Forms

Tom Weston

Abstract. Let $\rho\colon G_{\mathbf{Q}} \to \mathrm{GL}_n(\mathbf{Q}_\ell)$ be a motivic ℓ-adic Galois representation. For fixed $m > 1$ we initiate an investigation of the density of the set of primes p such that the trace of the image of an arithmetic Frobenius at p under ρ is an m-th power residue modulo p. Based on numerical investigations with modular forms we conjecture (with Ramakrishna) that this density equals $1/m$ whenever the image of ρ is open. We further conjecture that for such ρ the set of these primes p is independent of any set defined by Cebatorev-style Galois-theoretic conditions (in an appropriate sense). We then compute these densities for certain m in the complementary case of modular forms of CM-type with rational Fourier coefficients; our proofs are a combination of the Cebatorev density theorem (which does apply in the CM case) and reciprocity laws applied to Hecke characters. We also discuss a potential application (suggested by Ramakrishna) to computing inertial degrees at p in abelian extensions of imaginary quadratic fields unramified away from p.

Let $f = \sum a_n q^n$ be a newform of weight $k \geq 2$ with rational Fourier coefficients. For an integer $m \geq 2$ let $\delta_m(f)$ denote the relative density (assuming that it exists) of the set

$$\{p \equiv 1 \,(\mathrm{mod}\, m)\ ;\ a_p \text{ is a non-zero } m\text{-th power modulo } p\} \tag{0.1}$$

inside the set of primes $p \equiv 1 \,(\mathrm{mod}\, m)$ such that a_p is non-zero modulo p. Based on computations with various newforms we make the following conjecture.

Conjecture *The density $\delta_m(f)$ exists. It equals $\frac{1}{m}$ unless f has complex multiplication and m is not relatively prime to $6(k-1)$.*

In fact, we suspect that much more is true: we conjecture that this relative density does not change after restriction to any set of primes defined by a Cebatorev-style Frobenius condition; that is, we expect that the sets (0.1) yield sets of primes of positive density which are quite different from those sets determined by Galois-theoretic conditions. See Conjecture 1.2 for a precise statement.

For CM-forms f and some m dividing $6(k-1)$, the set (0.1) is in fact defined by Galois-theoretic conditions. We use this to prove the following result; see Theorems 3.3, 4.2, and 4.3 for precise statements. (In particular, Theorem 3.3 includes the cases $d = 1, 3$ when $m = 2$.)

Theorem *Let $K = \mathbf{Q}(\sqrt{-d})$ be an imaginary quadratic field with odd class number h. Fix $k \geq 2$, $k \equiv 1 \,(\mathrm{mod}\, h)$, and let $S_k^{K-\mathrm{cm}}(\mathbf{Q})$ denote the set of newforms of weight k with rational coefficients and complex multiplication by K.*

Received by the editors October 14, 2003; revised December 2, 2003.
AMS subject classification: Primary: 11F30; secondary: 11G15, 11A15.
©Canadian Mathematical Society 2005.

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

(1) *Assume that* $d \neq 1, 3$ *and* k *even. Then* $\delta_2(f) = \frac{1}{2}$ *for all but two* $f \in S_k^{K-\mathrm{cm}}(\mathbf{Q})$*; for these two forms,* $\delta_2(f)$ *equals* $\frac{1}{4}$ *or* $\frac{3}{4}$.
(2) *Assume that* $d \neq 1, 3$ *and* k *odd. Then* $\delta_2(f) = \frac{3}{4}$ *for all but two* $f \in S_k^{K-\mathrm{cm}}(\mathbf{Q})$*; for these two forms,* $\delta_2(f)$ *equals* $\frac{1}{2}$ *or* 1.
(3) *Assume that* $d = 3$*. Then* $\delta_3(f)$ *equals either* $\frac{5}{9}$ *or* 1 *for* $f \in S_k^{K-\mathrm{cm}}(\mathbf{Q})$.
(4) *Assume that* $d > 3$*. Then for any* $m \mid k-1$ *we have* $\delta_m(f) = \frac{3}{4}$ *for all but finitely many forms* $f \in S_k^{K-\mathrm{cm}}(\mathbf{Q})$*; for these exceptional forms,*$\delta_m(f)$ *equals either* $\frac{1}{2}$ *or* 1.

We fully expect that similar results can be proven for imaginary quadratic fields with even class number, but our methods here require the class number to be odd for a key step when a Legendre symbol is raised to the h-th power.

The original motivation for this work was the following question of Ramakrishna: If E is an elliptic curve over $\mathbf{Q}$, are the Fourier coefficients $a_p(E) := p + 1 - \#E(\mathbf{F}_p)$ cubes for infinitely many $p \equiv 1 \pmod 3$? This question in turn was motivated by the following observation of Ramakrishna (in the case $m = 3$), which we discuss in detail in Section 2.3.

Proposition *Let* K *be an imaginary quadratic field of class number one and let* m *be a prime relatively prime to* $\#\mathcal{O}_K^\times$*. Let* $p \equiv 1 \pmod m$ *be a prime greater than* 3 *which splits in* $K/\mathbf{Q}$ *and let* K_p^m *be the maximal abelian* m*-extension of* K *which is unramified away from* p*. Then* p *has inertial degree one in* $K_p^m/\mathbf{Q}$ *if and only if* $a_p(E)$ *is an* m*-th power modulo* p*, where* E *is any rational elliptic curve with complex multiplication by* K *and good reduction at* p.

In fact, one can state the above criterion in terms of modular forms of higher weight as well; see Remark 2.9. Unfortunately, our methods do not yield a single case in which we can show that the criterion of the proposition is satisfied for infinitely many p.

In Section 1 we formulate our precise conjectures and discuss the numerical evidence. In Section 2 we begin the study of the CM-case, relating the power residues of Fourier coefficients of CM-forms to power residues of the associated Hecke character. In Section 3 we combine this formula with the quadratic reciprocity law to compute $\delta_2(f)$ for CM-forms f. We consider the cases $d = m = 3$ and $m \mid k-1$ for f of weight k in Section 4.

We remark that the methods of this paper are essentially elementary. We suspect that it will require much deeper methods to make any progress on our conjectures in the general case.

Notation

For $m \geq 2$ and $\mathfrak{p}$ a prime of a number field K with residue field of order q congruent to 1 modulo m we write $\left(\frac{\cdot}{\mathfrak{p}}\right)_m$ for the m-th power residue symbol modulo $\mathfrak{p}$; thus for $\alpha \in \mathcal{O}_K$, $\alpha \notin \mathfrak{p}$, we have $\left(\frac{\alpha}{\mathfrak{p}}\right)_m \in \mu_m$,

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_m \equiv \alpha^{(q-1)/m} \pmod{\mathfrak{p}},$$

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

and $\left(\frac{\alpha}{\mathfrak{p}}\right)_m = 1$ if and only if α is a non-zero m-th power residue modulo $\mathfrak{p}$. We simply write $\left(\frac{\alpha}{\mathfrak{p}}\right)$ in the case $m = 2$.

By a *Hecke character* over a number field K we mean a continuous homomorphism

$$\chi\colon \mathbf{A}_K^\times / K^\times \to \bar{\mathbf{Q}}^\times$$

with $\mathbf{A}_K$ the adeles of K. We say that χ is *unramified* at a prime $\mathfrak{p}$ of $\mathcal{O}_K$ if $\chi(\mathcal{O}_{K_\mathfrak{p}}^\times) = 1$ (where we embed the completion $K_\mathfrak{p}^\times$ of K at $\mathfrak{p}$ into $\mathbf{A}_K^\times$ in the obvious manner). In this case we write $\chi(\mathfrak{p})$ for the value of χ on any uniformizer of $K_\mathfrak{p}$ and we extend χ to a character on all unramified fractional ideals in the obvious way.

If $\mathcal{P}$ is a set of primes, by the *density* of $\mathcal{P}$ we always mean the Dirichlet density, although all results in this paper remain true for natural density as well. For $\alpha \in \mathbf{Q}^\times$ we write $D(\alpha)$ for the discriminant of $\mathbf{Q}(\sqrt{\alpha})$ over $\mathbf{Q}$.

1 Conjectures

1.1 Galois Representations

Consider a Galois representation

$$\rho\colon \operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_n(\mathbf{Q}_\ell).$$

Suppose that ρ is *motivic* in the sense that there is a smooth, projective variety X over $\mathbf{Q}$ and a projector p in the ring of algebraic correspondences on X such that ρ is the Galois representation on

$$p_* H^i_{\text{ét}}\left(X_{\bar{\mathbf{Q}}}, \mathbf{Q}_\ell(j)\right)$$

for some i, j. (According to the Fontaine–Mazur conjectures [4] it should be equivalent to suppose that ρ is finitely ramified and potentially semistable at ℓ.) It follows from Deligne's proof of the Weil conjectures [2] that

$$a_p(\rho) := \operatorname{tr} \rho(\mathrm{Frob}_p)$$

is a rational integer for almost all primes p, independent of the choice of arithmetic Frobenius element Frob_p.

For an integer $m \geq 2$, define

$$\delta_m(\rho) = \frac{\text{density of } \left\{ p \equiv 1 \,(\mathrm{mod}\, m)\ ;\ \left(\frac{a_p(\rho)}{p}\right)_m = 1 \right\}}{\text{density of } \left\{ p \equiv 1 \,(\mathrm{mod}\, m)\ ;\ a_p(\rho) \not\equiv 0 \,(\mathrm{mod}\, p) \right\}}$$

if these densities exist. With Ramakrishna, we make the following conjecture.

Conjecture 1.1 *Let ρ be a motivic Galois representation as above. If the image of ρ is open, then*

$$\delta_m(\rho) = \frac{1}{m}.$$

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

We remark that Conjecture 1.1 is certainly false for many infinitely ramified Galois representations, as by [6] it is possible to control the Frobenius polynomials (and thus the $a_p(\rho)$) at a set of primes of density one.

Note that when ρ has open image, one expects the set of primes p which divide $a_p(\rho)$ to have density zero, so that $\delta_m(\rho)$ should be an absolute density in this case.

Of course, one could attempt to formulate an analogous conjecture for Galois representations of number fields taking values in larger ℓ-adic fields. We have not attempted to do so here; we only point out that the density $\delta_m(\rho)$ is certainly dependent on the choice of coefficient field, so that the conjectures must be somewhat more complicated in the general case.

1.2 Fourier Coefficients of Modular Forms

The motivation for Conjecture 1.1 comes from numerical investigations with Fourier coefficients of modular forms. Let $f = \sum a_n q^n$ be a newform of weight $k \geq 2$ and level N with rational Fourier coefficients. For any prime ℓ Deligne has constructed a motivic Galois representation

$$\rho_f \colon \operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{Q}_\ell)$$

with the property that $\operatorname{tr} \rho_f(\mathrm{Frob}_p) = a_p$ for $p \nmid N\ell$; see [10], for example. By [8, Theorem 5.7] the image of ρ_f is open provided that f is not of CM-type.

We briefly discuss the numerical evidence for Conjecture 1.1 for the representations ρ_f; we simply write $\delta_m(f)$ for $\delta_m(\rho_f)$ in this case, or $\delta_m(E)$ if f is the newform corresponding to a rational elliptic curve E. For integers $P_1 < P_2$ define

$$\delta_m(f; P_1, P_2) = \frac{\#\left\{ p \equiv 1 \,(\mathrm{mod}\, m) \,;\, \left(\frac{a_p}{p}\right)_m = 1, \quad P_1 \leq p \leq P_2 \right\}}{\#\{p \equiv 1 \,(\mathrm{mod}\, m) \,;\, a_p \not\equiv 0 \,(\mathrm{mod}\, p), \quad P_1 \leq p \leq P_2\}}.$$

We have computed:

(1) $\delta_m(E; 10^8, 2{\cdot}10^8)$ for $m \leq 10$ and various rational elliptic curves of small conductor;
(2) $\delta_m(f; 1, 1000)$ for $m \leq 10$ and various modular forms f of weight at least 3 contained in the tables [12];
(3) $\delta_m(\Delta; 10^6, 2 \cdot 10^6)$ for $m \leq 10$ and the modular form $\Delta = \sum \tau(n) q^n$ with $\tau(n)$ the Ramanujan τ-function.

In each case we obtained results consistent with Conjecture 1.1. To give a single example, we report the information obtained for the elliptic curve $E = X_0(11)$. The data reported below are for the set of primes

$$\{p \equiv 1 \,(\mathrm{mod}\, m) \,;\, 10^8 \leq p \leq 2 \cdot 10^8\}.$$

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

m	#p s.t. $\left(\frac{a_p}{p}\right)_m = 1$	#p s.t. $p \nmid a_p$	$\delta_m(E; 10^8, 2\cdot 10^8)$
2	2662953	5317482	0.5008
3	888792	2658461	0.3343
4	667722	2658316	0.2512
5	266666	1329469	0.2006
6	446913	2658461	0.1681
7	127203	886591	0.1435
8	168427	1329053	0.1267
9	99178	886298	0.1119
10	133116	1329469	0.1001

S. Wong has pointed out that in most cases the data appear to be slightly biased, so that the approximate densities are usually larger than $\frac{1}{m}$. For the case of elliptic curves this may be at least partially explained by the fact that $|a_p| \leq 2\sqrt{p}$ and such small values are slightly more likely to be power residues. In any event, Conjecture 1.1 asserts that in the limit these biases disappear.

1.3 Cebatorev Sets

We have also computed densities as above for sets of primes satisfying additional congruence conditions (that is, with prescribed splitting in cyclotomic fields) and with specified inertial degrees in splitting fields of various cubic polynomials. These computations suggest a stronger statement than Conjecture 1.1. For ρ a motivic Galois representation as above and for $\mathcal{P}$ a set of rational primes of positive density, we define

$$\delta_m(\rho;\mathcal{P}) = \frac{\text{density of } \left\{ p \equiv 1 \,(\mathrm{mod}\, m)\ ;\ \left(\frac{a_p(\rho)}{p}\right)_m = 1 \right\} \cap \mathcal{P}}{\text{density of } \{p \equiv 1 \,(\mathrm{mod}\, m)\ ;\ a_p \not\equiv 0 \,(\mathrm{mod}\, p)\} \cap \mathcal{P}}$$

if these densities exist. We say that such a set $\mathcal{P}$ is a *Cebatorev set* if there is a finite Galois extension K of $\mathbf{Q}$ and a subset $S \subseteq \mathrm{Gal}(K/\mathbf{Q})$, stable under conjugation, such that, up to finite sets, $\mathcal{P}$ is the set of primes p with $\mathrm{Gal}(K/\mathbf{Q})$-Frobenius lying in S.

Conjecture 1.2 *Let ρ be a motivic Galois representation with open image as above. Then for any Cebatorev set $\mathcal{P}$,*

$$\delta_m(\rho;\mathcal{P}) = \frac{1}{m}.$$

Conjecture 1.2 essentially asserts that the sets

$$\left\{ p \equiv 1 \,(\mathrm{mod}\, m)\ ;\ \left(\frac{a_p(\rho)}{p}\right)_m = 1 \right\} \tag{1.1}$$

can not be described in terms of Cebatorev sets. If Conjecture 1.2 holds, it would thus yield an entirely new collection of naturally occurring sets of primes of positive density.

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

1.4 CM-Representations

The case where ρ has smaller image in $\mathrm{GL}_n(\mathbf{Q}_\ell)$ does not appear to admit a uniform statement such as Conjecture 1.1. We do not speculate on the form of a general conjecture. However, in certain cases we expect that the analogous result holds.

Conjecture 1.3 *Let f be a rational newform of weight $k \geq 2$ with complex multiplication by the field $\mathbf{Q}(\sqrt{-d})$. If $d \neq 3$ and m is relatively prime to $2(k-1)$, or if $d = 3$ and m is relatively prime to $6(k-1)$, then*

$$\delta_m(f) = \frac{1}{m}.$$

In the remainder of the paper we consider the exceptional cases $m = 2$ and $m \mid k-1$ (and $m = d = 3$). In these cases we will see that, in contrast to Conjecture 1.2, (1.1) is a Cebatorev set and thus that we can compute its density. (Roughly speaking, the case $m = 2$ is exceptional due to the relation between CM modular forms and quadratic fields, while the case $m \mid k-1$ is exceptional due to the relation between a CM form of weight k and the $(k-1)^{\text{st}}$ power of a Hecke character.)

2 Modular Forms of CM-Type with Rational Fourier Coefficients

For the remainder of the paper we fix an imaginary quadratic field K with ring of integers $\mathcal{O}$. We write d for the unique squarefree integer such that $K = \mathbf{Q}(\sqrt{-d})$, D for the discriminant of K, and w for the order of $\mathcal{O}^\times$. For $\alpha \in K$, we write $\bar{\alpha}$ for the conjugate of α.

Let H denote the Hilbert class field of K, so that $[H:K]$ equals the class number h of K. We always assume that h is odd, so that either $d \in \{1, 2\}$ or $d \equiv 3 \pmod 4$. For later use we set $\varepsilon = 2$ (resp., $\varepsilon = -1$, resp., $\varepsilon = 1$) for $d = 1$ (resp., $d \equiv 3 \pmod 8$, resp., $d \equiv 7 \pmod 8$ or $d = 2$).

2.1 Hecke Characters

By [5, Section 11.2], for $d > 3$ there is a unique Hecke character

$$\psi' \colon \mathbf{A}_H^\times / H^\times \to K^\times,$$

unramified away from D, with the property that for any prime $\mathfrak{P}$ of $\mathcal{O}_H$ (relatively prime to D) $\psi'(\mathfrak{P})$ is the unique generator of the principal ideal $N_{H/K}\mathfrak{P}$ which is a square modulo $\sqrt{-d}$. (Note that $w = 2$ and $d \equiv 3 \pmod 4$, so that there is indeed a unique such generator.) Since $\psi' \circ \sigma$ has the same property for any $\sigma \in \mathrm{Gal}(H/K)$, the Hecke character ψ' is invariant under the action of $\mathrm{Gal}(H/K)$ on $\mathbf{A}_H^\times / H^\times$.

Define a Hecke character $\psi \colon \mathbf{A}_K / K^\times \to K^\times$ as the composition

$$\mathbf{A}_K^\times / K^\times \to \mathbf{A}_H^\times / H^\times \xrightarrow{\psi'} K^\times;$$

it follows from Lemma 2.1 below that ψ has infinity type $(h, 0)$ (in the sense of [3, Section II.1.1]).

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

Lemma 2.1 *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ relatively prime to D. Then $\psi(\mathfrak{p})$ is the unique generator of $\mathfrak{p}^h$ which is a square modulo $\sqrt{-d}$.*

Proof Let $\varpi_{\mathfrak{p}} \in \mathbf{A}_K^{\times}$ be an idele which is trivial away from $\mathfrak{p}$ and which is a uniformizer at $\mathfrak{p}$. Then the image of $\varpi_{\mathfrak{p}}$ in $\mathbf{A}_H^{\times}$ can be written as $\varpi_{\mathfrak{P}_1} \cdots \varpi_{\mathfrak{P}_g}$ for analogously defined ideles $\varpi_{\mathfrak{P}_i}$; here $\mathfrak{p}\mathcal{O}_H = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ is the decomposition of $\mathfrak{p}$ into primes of $\mathcal{O}_H$. Since ψ' is $\mathrm{Gal}(H/K)$-invariant it follows that

$$\psi(\mathfrak{p}) = \psi'(\mathfrak{P}_1) \cdots \psi'(\mathfrak{P}_g) = \psi'(\mathfrak{P}_1)^g.$$

As $\psi'(\mathfrak{P}_1)\mathcal{O}_K = N_{H/K}\mathfrak{P}_1 = \mathfrak{p}^{h/g}$, we conclude that $\psi(\mathfrak{p})\mathcal{O}_K = \mathfrak{p}^h$. Each $\psi'(\mathfrak{P}_i)$ is a square modulo $\sqrt{-d}$, so that the same is true of $\psi(\mathfrak{p})$; thus $\psi(\mathfrak{p})$ is the unique generator of $\mathfrak{p}^h$ which is a square modulo $\sqrt{-d}$, as claimed. ∎

We define the Hecke character $\psi\colon \mathbf{A}_K^{\times}/K^{\times} \to K^{\times}$ for $d = 1$ (resp., $d = 2$, resp., $d = 3$) as the Hecke character over K associated (as in [11, Theorem 9.2]) to the $\mathbf{Q}$-isogeny class of the elliptic curve $32A$ (resp., $256D$, resp., $27A$) of [1].

Lemma 2.2 *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ relatively prime to D. Then for $d = 1$ (resp., $d = 3$) $\psi(\mathfrak{p})$ is the unique generator of $\mathfrak{p}$ which is congruent to 1 modulo $2 + 2i$ (resp., modulo 3). For $d = 2$, $\psi(\mathfrak{p})$ is the unique generator of $\mathfrak{p}$ which is congruent to one of*

$$\left\{1, 3, 5 + \sqrt{-2}, 7 + \sqrt{-2}, 5 + 2\sqrt{-2}, 7 + 2\sqrt{-2}, 5 + 3\sqrt{-2}, 7 + 3\sqrt{-2}\right\} \tag{2.1}$$

modulo $4\sqrt{-2}$.

Proof This is well-known for $d = 1, 3$; see for example [11, Example II.10.6 and Exercise II..34]. For $d = 2$, by [11, Proposition 10.4] $\psi(\mathfrak{p})$ is a generator of $\mathfrak{p}$ for all $\mathfrak{p} \neq \sqrt{-2}\mathcal{O}$. Since ψ has conductor dividing $\sqrt{256} = 16$, to determine ψ, it suffices to determine the sign of this generator for the principal ideals generated by representatives for all classes in $(\mathcal{O}/16\mathcal{O})^{\times}$. This is straightforward via [11, Corollary 10.4.1] and results in the characterization given above. ∎

Definition 2.3 For any $\alpha \in \mathbf{Q}^{\times}$ and any $k \geq 2$ which is congruent to 1 modulo h, let

$$\psi_{\alpha}^k\colon \mathbf{A}_K^{\times}/K^{\times} \to K^{\times}$$

denote the Hecke character unramified away from D and α such that

$$\psi_{\alpha}^k(\mathfrak{p}) = \psi(\mathfrak{p})^{(k-1)/h} \cdot \left(\frac{\varepsilon}{\mathfrak{p}}\right)_w^{(k-1)/h} \cdot \left(\frac{\alpha}{\mathfrak{p}}\right)_w$$

for any $\mathfrak{p}$ relatively prime to D and α.

The extra twist by ε is included to simplify the statements below. Note that ψ_{α}^k has infinity type $(k-1, 0)$.

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

2.2 Modular Forms

Fix $k \geq 2$, $k \equiv 1 \pmod{h}$, and $\alpha \in \mathbf{Q}^\times$. By [8, Theorem 3.4] the Fourier series

$$g_\alpha^k := \sum_{(\mathfrak{a},D)=(\mathfrak{a},\alpha)=1} \psi_\alpha^k(\mathfrak{a}) q^{\mathbf{N}\mathfrak{a}}$$

(summing over ideals of $\mathcal{O}$ prime to D and α) is a cusp form of weight k for $\Gamma_1(\mathbf{N}\mathfrak{m})$ (with $\mathfrak{m}$ the conductor of ψ_α^k) which is an eigenform for the Hecke operators T_n with n prime to D and α.

Definition 2.4 Let

$$f_\alpha^k = \sum a_n(f_\alpha^k) q^n$$

denote the normalized newform associated to g_α^k; we have $a_n(f_\alpha^k) = a_n(g_\alpha^k)$ for n prime to D and α.

We claim that f_α^k has rational Fourier coefficients. Indeed, for p relatively prime to D and α, Lemmas 2.1 and 2.2 show that $\psi_\alpha^k(\bar{\mathfrak{p}}) = \overline{\psi_\alpha^k(\mathfrak{p})}$, so that

$$a_p(f_\alpha^k) = \psi_\alpha^k(\mathfrak{p}) + \psi_\alpha^k(\bar{\mathfrak{p}}) \in \mathbf{Q}. \tag{2.2}$$

By [8, Corollary 3.1] the $a_p(f_\alpha^k)$ for almost all primes p generate the field of all Fourier coefficients of f_α^k, so that the rationality of $a_n(f_\alpha^k)$ for all $n \geq 1$ follows.

Note that $f_\alpha^k = f_{-d\alpha}^k$, but otherwise the f_α^k are all distinct. (This can perhaps be seen most easily by considering the restriction of the Galois representation associated to f_α^k to the field $\mathbf{Q}(\sqrt{-d})$.) In fact, any modular form of weight $k \equiv 1 \pmod{h}$ with complex multiplication by K and with rational Fourier coefficients is equal to f_α^k for some $\alpha \in \mathbf{Q}^\times$, although we will not prove this here. (In general there may also be such forms of weights congruent to 1 modulo the exponent of the class group of $\mathcal{O}$, but these are the only other possible weights.)

The next lemma gives the relation between the power residues of the Fourier coefficients of the CM-form f_α^k and the values of the Hecke character ψ_α^k.

Lemma 2.5 *Fix $m \geq 1$, $k \geq 2$, $k \equiv 1 \pmod{h}$, and $\alpha \in \mathbf{Q}^\times$. Let p be a rational prime such that:*

(1) *$p \equiv 1 \pmod{m}$;*
(2) *p splits as $\mathfrak{p}\bar{\mathfrak{p}}$ in $K/\mathbf{Q}$;*
(3) *p is relatively prime to α.*

Then

$$\left(\frac{a_p(f_\alpha^k)}{p}\right)_m = \left(\frac{\psi_\alpha^k(\mathfrak{p})}{\bar{\mathfrak{p}}}\right)_m.$$

Proof Since $\bar{\mathfrak{p}}$ has norm p we have by (2.2) that

$$\left(\frac{a_p(f_\alpha^k)}{p}\right)_m = \left(\frac{\psi_\alpha^k(\mathfrak{p}) + \psi_\alpha^k(\bar{\mathfrak{p}})}{\bar{\mathfrak{p}}}\right)_m.$$

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

Note that by Lemmas 2.1 and 2.2 $\psi(\bar{\mathfrak{p}})$, and thus $\psi_\alpha^k(\bar{\mathfrak{p}})$, is divisible by $\bar{\mathfrak{p}}$. Thus

$$\left(\frac{\psi_\alpha^k(\mathfrak{p}) + \psi_\alpha^k(\bar{\mathfrak{p}})}{\bar{\mathfrak{p}}}\right)_m = \left(\frac{\psi_\alpha^k(\mathfrak{p})}{\bar{\mathfrak{p}}}\right)_m$$

and the lemma follows. ∎

2.3 Applications to Abelian Extensions of K

In this section we assume for simplicity that $h = 1$. Fix a prime m relatively prime to w (that is, m is odd and if $d = 3$ then we also require $m \neq 3$) and fix $p \equiv 1 \pmod{m}$ which splits as $\mathfrak{p}\bar{\mathfrak{p}}$ in $K/\mathbf{Q}$; assume also that $p > 3$. Let K_p^m denote the maximal abelian extension of K of exponent m which is unramified away from $\mathfrak{p}$ and $\bar{\mathfrak{p}}$.

One can construct K_p^m via the Hecke character ψ as follows. Let $\tilde{\psi}_p \colon G_K \to \mathcal{O}_p^\times$ be the p-adic Galois character associated to ψ via class field theory. Let

$$\bar{\psi}_p \colon G_K \to (\mathcal{O}/p)^\times \cong \mathbf{F}_p^\times \times \mathbf{F}_p^\times$$

be the reduction of $\tilde{\psi}_p$ (which is surjective by [9, Corollary 5.20]) and let

$$\bar{\psi}_p^m \colon G_K \twoheadrightarrow (\mathbf{Z}/m\mathbf{Z})^2$$

denote the composition of $\bar{\psi}_p$ with some fixed surjection $(\mathcal{O}/p)^\times \twoheadrightarrow (\mathbf{Z}/m\mathbf{Z})^2$. We write $K(\bar{\psi}_p)$ and $K(\bar{\psi}_p^m)$ for the fixed fields of the kernels of these characters. Note that $K(\bar{\psi}_p)$ is equal to $K(E[p])$ with E a rational elliptic curve corresponding to ψ over K.

Lemma 2.6 *With notation as above, $K_p^m = K(\bar{\psi}_p^m)$.*

Proof By [11, Theorem II.5.6] the field $K(\bar{\psi}_p)$ contains the ray class field of K of conductor p, so that it certainly contains K_p^m. Since $K(\bar{\psi}_p^m)$ is the maximal subextension of $K(\bar{\psi}_p)/K$ of exponent m, to prove the lemma it thus suffices to show that $K(\bar{\psi}_p^m)/K$ is unramified away from $\mathfrak{p}$ and $\bar{\mathfrak{p}}$. To see this, note that $K(\bar{\psi}_p)/K$ is unramified away from Dp since ψ is unramified away from D. Furthermore, by [9, Theorem 5.15] the image under $\tilde{\psi}_p$ of an inertia group at a prime dividing D has order dividing w. Since we are requiring m to be relatively prime to w, it follows that $K(\bar{\psi}_p^m)/K$ must be unramified at all such primes, which completes the proof. ∎

It follows from Lemma 2.6 that

$$\mathrm{Gal}(K_p^m/K) \cong (\mathbf{Z}/m\mathbf{Z})^2.$$

In particular, K_p^m is a Galois extension of $\mathbf{Q}$ of degree $2m^2$; thus

$$e_p f_p g_p = 2m^2$$

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

where e_p (resp., f_p, resp., g_p) is the ramification index (resp., inertial degree, resp., splitting degree) of p in $K_p^m/\mathbf{Q}$. Since K has no everywhere unramified extensions, $K_p^m/\mathbf{Q}$ must be ramified at p and since $p \neq m$ the inertia groups at p must be cyclic (as the tame inertia group of $\mathbf{Q}_p$ is pro-cyclic); as m is prime it follows that $e_p = m$. Since 2 divides g_p, it follows that there are two possibilities:

$$e_p = m, \quad f_p = m, \quad g_p = 2$$

or

$$e_p = m, \quad f_p = 1, \quad g_p = 2m.$$

The next proposition shows that one can determine which of these occurs in terms of the power residue of the p-th Fourier coefficient of E.

Proposition 2.7 *Let E be a rational elliptic curve with Hecke character ψ over K. For $p \equiv 1 \pmod{m}$ greater than 3 and split in $K/\mathbf{Q}$, we have $f_p = 1$ if and only if $\left(\frac{a_p(E)}{p}\right)_m = 1$.*

Proof Since

$$\mathrm{Gal}(K(E[p])/K) \cong (\mathcal{O}/p)^\times \cong (\mathbf{Z}/(p-1)\mathbf{Z})^2$$

and

$$\mathrm{Gal}(K_p^m/K) \cong \mathrm{Gal}(K(E[p])/K)/m \cdot \mathrm{Gal}(K(E[p])/K),$$

one sees easily that $f_p = 1$ if and only if the inertial degree of $\mathbf{Q}_p(E[p])/\mathbf{Q}_p$ divides $(p-1)/m$. The latter condition is equivalent to the p-torsion of E over $\bar{\mathbf{F}}_p$ being defined over $\mathbf{F}_{p^{(p-1)/m}}$. Since E is ordinary at p (as p splits in $K/\mathbf{Q}$) and thus has one-dimensional p-torsion over $\bar{\mathbf{F}}_p$, it follows that to prove the proposition it suffices to show that $\left(\frac{a_p(E)}{p}\right)_m = 1$ if and only if p divides $\#E(\mathbf{F}_{p^{(p-1)/m}})$.

Let α, β be the p-adic roots of the Frobenius polynomial

$$x^2 - a_p(E)x + p;$$

since E is ordinary at p we may choose α, β so that α is a p-adic unit and β is divisible by p. In particular,

$$\alpha \equiv a_p(E) \pmod{p}.$$

By the Riemann hypotheses for elliptic curves over finite fields we have

$$\begin{aligned}\#E(\mathbf{F}_{p^{(p-1)/m}}) &= p^{(p-1)/m} + 1 - \alpha^{(p-1)/m} - \beta^{(p-1)/m} \\ &\equiv 1 - a_p(E)^{(p-1)/m} \pmod{p}.\end{aligned}$$

Since

$$a_p(E)^{(p-1)/m} \equiv \left(\frac{a_p(E)}{p}\right)_m \pmod{p},$$

the proposition follows from this. ∎

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

Remark 2.8 If m is not relatively prime to w, then one can easily obtain the analogue of Proposition 2.7 via Kummer theory.

Remark 2.9 Fix $k \geq 2$ and $\alpha \in \mathbf{Q}^{\times}$. If $k-1$ is relatively prime to m (which in turn is still assumed relatively prime to w), then it follows from Lemma 2.5 that

$$\left(\frac{a_p(f_\alpha^k)}{p}\right)_m = \left(\frac{a_p(E)}{p}\right)_m.$$

Thus one can also compute f_p via the Fourier coefficients of f_α^k. (In particular, this shows that it does not matter which rational elliptic curve with complex multiplication by K one uses in Proposition 2.7.) Unfortunately, the various hypotheses on m and k above rule out any case in which we are able to calculate $\left(\frac{a_p(f_\alpha^k)}{p}\right)_m$.

Remark 2.10 When considering Proposition 2.7 for $a_p(f_\alpha^k)$ as above, it is perhaps somewhat more enlightening to regard $\mathrm{Gal}(K_p^m/K)$ as a quotient of the mod p Galois representation associated to f_α^k; Proposition 2.7 can then be recovered from the fact that the restriction of this Galois representation to a decomposition group at p has the form

$$\begin{pmatrix} \chi^{k-1}\varphi^{-1} & * \\ 0 & \varphi \end{pmatrix}$$

with χ the cyclotomic character and φ an unramified character with the property that

$$\varphi(\mathrm{Frob}_p) \equiv a_p(f_\alpha^k) \pmod{p}.$$

3 Squares

3.1 Preliminaries

In order to determine the quadratic character of Hecke characters over imaginary quadratic fields with odd class number we will need the following result. Recall that $\varepsilon = -1$ (resp., $\varepsilon = 1$) if $d \equiv 3 \pmod 8$ (resp., $d \equiv 7 \pmod 8$).

Lemma 3.1 *Let p be a prime which splits as $\mathfrak{p}\bar{\mathfrak{p}}$ in $K/\mathbf{Q}$ and let π be a generator of $\mathfrak{p}^h$. (If $d = 1$, further assume that $\pi \equiv 1 \pmod{2+2i}$.)*

(1) *If $p \equiv 1 \pmod 4$, then*

$$\left(\frac{\pi}{\bar{\mathfrak{p}}}\right) = \left(\frac{-d}{p}\right)_4.$$

(2) *If $d \neq 2$ and $p \equiv 3 \pmod 4$, then*

$$\left(\frac{\pi}{\bar{\mathfrak{p}}}\right) = \varepsilon\left(\frac{\pi}{\sqrt{-d}}\right).$$

(3) *If $d = 2$ and $p \equiv 3 \pmod 4$, then $\left(\frac{\pi}{\bar{\mathfrak{p}}}\right) = 1$ if and only if π is congruent to an element of (2.1) modulo $4\sqrt{-2}$.*

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

Proof Write $\pi = a + b\sqrt{-d}$ with $a, b \in \frac{1}{2}\mathbf{Z}$; if we write $a = 2^r a'$, $b = 2^s b'$ with a', b' odd integers, then $r = -1$ if and only if $s = -1$.

We assume first that $p \equiv 1 \pmod 4$. Since $\bar{\pi} \in \bar{\mathfrak{p}}$, we have

$$\left(\frac{\pi}{\bar{\mathfrak{p}}}\right) = \left(\frac{\pi - \bar{\pi}}{\bar{\mathfrak{p}}}\right) = \left(\frac{2b\sqrt{-d}}{\bar{\mathfrak{p}}}\right) = \left(\frac{2b}{\bar{\mathfrak{p}}}\right)\left(\frac{\sqrt{-d}}{\bar{\mathfrak{p}}}\right). \tag{3.1}$$

Since $2b$ is an integer and $\bar{\mathfrak{p}}$ has norm p, we have

$$\left(\frac{2b}{\bar{\mathfrak{p}}}\right) = \left(\frac{2b}{p}\right) = \left(\frac{2}{p}\right)^{s+1}\left(\frac{b'}{p}\right).$$

By quadratic reciprocity and the fact that h is odd we have

$$\left(\frac{b'}{p}\right) = \left(\frac{p}{b'}\right) = \left(\frac{p^h}{b'}\right) = \left(\frac{a^2 + db^2}{b'}\right) = \left(\frac{a^2}{b'}\right) = 1.$$

As $\left(\frac{\sqrt{-d}}{\mathfrak{p}}\right) = \left(\frac{-d}{p}\right)_4$ by (3.1) we conclude that

$$\left(\frac{\pi}{\bar{\mathfrak{p}}}\right) = \left(\frac{2}{p}\right)^{s+1}\left(\frac{-d}{p}\right)_4. \tag{3.2}$$

If $p \equiv 1 \pmod 8$ this completes the proof. If $p \equiv 5 \pmod 8$, then one shows easily (using that $\pi \equiv 1 \pmod{2+2i}$ in the case $d = 1$) that $s = \pm 1$; thus (3.2) completes the proof in this case as well.

Next assume $p \equiv 3 \pmod 4$; in particular, we now have $d \neq 1$. We have

$$\left(\frac{\pi}{\bar{\mathfrak{p}}}\right) = \left(\frac{\pi + \bar{\pi}}{\bar{\mathfrak{p}}}\right) = \left(\frac{2a}{\bar{\mathfrak{p}}}\right) = \left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right)^{r+1}\left(\frac{a'}{p}\right).$$

Using quadratic reciprocity and the fact that h is odd, we obtain

$$\begin{aligned}\left(\frac{\pi}{\bar{\mathfrak{p}}}\right) &= \left(\frac{2}{p}\right)^{r+1}\left(\frac{-1}{a'}\right)\left(\frac{p}{a'}\right) = \left(\frac{2}{p}\right)^{r+1}\left(\frac{-1}{a'}\right)\left(\frac{p^h}{a'}\right) \\ &= \left(\frac{2}{p}\right)^{r+1}\left(\frac{-1}{a'}\right)\left(\frac{a^2 + db^2}{a'}\right) = \left(\frac{2}{p}\right)^{r+1}\left(\frac{-1}{a'}\right)\left(\frac{d}{a'}\right).\end{aligned} \tag{3.3}$$

For $d \neq 2$ we have $d \equiv 3 \pmod 4$, so that a second application of quadratic reciprocity now yields

$$\left(\frac{\pi}{\bar{\mathfrak{p}}}\right) = \left(\frac{2}{p}\right)^{r+1}\left(\frac{a'}{d}\right) = \left(\frac{2}{p}\right)^{r+1}\left(\frac{2}{d}\right)^{-r}\left(\frac{a}{d}\right).$$

If $p \equiv d \pmod 8$, then this immediately yields the lemma since $\left(\frac{2}{p}\right) = \left(\frac{2}{d}\right) = \varepsilon$. If $p \not\equiv d \pmod 8$, one finds easily that $r = \pm 1$; the lemma thus follows in this case as well.

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

When $d = 2$, one must have $p \equiv 3 \pmod 8$ and $r = s = 0$. In particular, π must be congruent to an element of

$$\{1+\sqrt{-2}, 3+\sqrt{-2}, 5+\sqrt{-2}, 7+\sqrt{-2}, 1+3\sqrt{-2}, 3+3\sqrt{-2}, 5+3\sqrt{-2}, 7+3\sqrt{-2}\}$$

modulo $4\sqrt{-2}$. By (3.3) we have

$$\left(\frac{\pi}{\bar{\mathfrak{p}}}\right) = \left(\frac{2}{p}\right)\left(\frac{-2}{a}\right) = -\left(\frac{-2}{a}\right),$$

which is 1 if and only if $a = 5, 7$. The lemma thus follows from the definition of (2.1). ∎

3.2 Densities

Combining Lemma 2.5 with Lemma 3.1 yields the following result on the quadratic character of the Fourier coefficients of the CM forms f_α^k.

Proposition 3.2 *Fix $k \geq 2$, $k \equiv 1 \pmod h$, and $\alpha \in \mathbf{Q}^\times$. Let p be a rational prime, relatively prime to α, which splits as $\mathfrak{p}\bar{\mathfrak{p}}$ in $K/\mathbf{Q}$.*

(1) *For $d \neq 1$,*

$$\left(\frac{a_p(f_\alpha^k)}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 4 \text{ and } k \text{ odd}; \\ \left(\frac{-d}{p}\right)_4 & p \equiv 1 \pmod 4 \text{ and } k \text{ even}; \\ \left(\frac{\alpha}{p}\right) & p \equiv 3 \pmod 4. \end{cases}$$

(2) *For $d = 1$,*

$$\left(\frac{a_p(f_\alpha^k)}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 8; \\ \left(\frac{\alpha}{p}\right) & p \equiv 5 \pmod 8. \end{cases}$$

Proof Assume first that $d \neq 1, 3$, so that $w = 2$. By Lemma 2.5 and the definition of ψ_α^k we have

$$\begin{aligned}\left(\frac{a_p(f_\alpha^k)}{p}\right) &= \left(\frac{\psi(\mathfrak{p})^{(k-1)/h} \cdot \left(\frac{\varepsilon}{\mathfrak{p}}\right)^{(k-1)/h} \cdot \left(\frac{\alpha}{\mathfrak{p}}\right)}{\bar{\mathfrak{p}}}\right) \\ &= \left(\frac{\psi(\mathfrak{p})}{\bar{\mathfrak{p}}}\right)^{(k-1)/h} \cdot \left(\frac{\left(\frac{\varepsilon}{p}\right)}{p}\right)^{(k-1)/h} \cdot \left(\frac{\left(\frac{\alpha}{p}\right)}{p}\right).\end{aligned}$$

When $p \equiv 1 \pmod 4$, the last two Legendre symbols above are trivial so that this yields

$$\left(\frac{a_p(f_\alpha^k)}{p}\right) = \left(\frac{\psi(\mathfrak{p})}{\bar{\mathfrak{p}}}\right)^{(k-1)/h} = \left(\frac{-d}{p}\right)_4^{(k-1)/h}$$

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

by Lemma 3.1 and the fact that $\psi(\mathfrak{p})$ generates $\mathfrak{p}^h$. Since $\left(\frac{-d}{p}\right)_4 = \pm 1$ (as p splits in K) and $(k-1)/h$ is even if and only if k is odd, the lemma follows in this case.

When $p \equiv 3 \pmod 4$ we instead obtain

$$\left(\frac{a_p(f_\alpha^k)}{p}\right) = \left(\frac{\psi(\mathfrak{p})}{\bar{\mathfrak{p}}}\right)^{(k-1)/h} \cdot \varepsilon^{(k-1)/h} \cdot \left(\frac{\alpha}{p}\right).$$

By Lemmas 2.1, 2.2 and 3.1 we have $\left(\frac{\psi(\mathfrak{p})}{\bar{\mathfrak{p}}}\right) = \varepsilon$, so that the lemma follows in this case as well.

The proof for $d = 3$ is similar using that

$$\left(\frac{\left(\frac{\alpha}{p}\right)_6}{\bar{\mathfrak{p}}}\right) = \begin{cases} 1 & p \equiv 1 \pmod{12}; \\ \left(\frac{\alpha}{p}\right) & p \equiv 7 \pmod{12}. \end{cases}$$

The proof for $d = 1$ also proceeds similarly, taking into account that $\varepsilon = 2$, that $\left(\frac{-1}{p}\right)_4 = 1$ for $p \equiv 1 \pmod 8$, and that

$$\left(\frac{\left(\frac{\alpha}{p}\right)_4}{\bar{\mathfrak{p}}}\right) = \begin{cases} 1 & p \equiv 1 \pmod 8; \\ \left(\frac{\alpha}{p}\right) & p \equiv 5 \pmod 8. \end{cases}$$

■

It is now a simple matter to determine the density of squares among the non-zero Fourier coefficients of f_α^k. By the definition of f_α^k we see that $a_p(f_\alpha^k) = 0$ for p inert in $K/\mathbf{Q}$ while $p \nmid a_p(f_\alpha^k)$ for p split in $K/\mathbf{Q}$ and relatively prime to α. Thus

$$\begin{aligned} \delta_2(f_\alpha^k) &:= \frac{\text{density of } \left\{p \,;\, \left(\frac{a_p(f_\alpha^k)}{p}\right) = 1\right\}}{\text{density of } \{p \,;\, a_p(f_\alpha^k) \not\equiv 0 \pmod p\}} \\ &= \frac{\text{density of } \left\{p \,;\, \left(\frac{a_p(f_\alpha^k)}{p}\right) = 1\right\}}{\text{density of } \{p \,;\, p \text{ split in } K/\mathbf{Q}\}} \\ &= 2 \cdot \left(\text{density of } \left\{p \,;\, \left(\frac{a_p(f_\alpha^k)}{p}\right) = 1\right\}\right) \end{aligned}$$

if this density is defined.

Theorem 3.3 *Fix $k \geq 2$, $k \equiv 1 \pmod h$, and $\alpha \in \mathbf{Q}^\times$.*

- *For $d \neq 1$ and k even*

$$\delta_2(f_\alpha^k) = \begin{cases} 3/4 & D(\alpha) \in \{1, D\}; \\ 1/4 & D(\alpha) \in \{-4, 4d\}; \\ 1/2 & \textit{otherwise.} \end{cases}$$

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

- *For $d \neq 1$ and k odd*

$$\delta_2(f_\alpha^k) = \begin{cases} 1 & D(\alpha) \in \{1, D\}; \\ 1/2 & D(\alpha) \in \{-4, 4d\}; \\ 3/4 & \textit{otherwise.} \end{cases}$$

- *For $d = 1$,*

$$\delta_2(f_\alpha^k) = \begin{cases} 1 & D(\alpha) \in \{1, -4\}; \\ 1/2 & D(\alpha) \in \{\pm 8\}; \\ 3/4 & \textit{otherwise.} \end{cases}$$

Proof We consider $d \neq 1$; the proof for $d = 1$ is handled in an entirely similar fashion, taking into account the different form of Proposition 3.2 in this case. Consider first primes $p \equiv 1 \pmod 4$, p relatively prime to α and split in $K/\mathbf{Q}$. These primes are (up to a finite set) precisely those which split completely in $\mathbf{Q}(\sqrt{-d}, i)/\mathbf{Q}$. By Proposition 3.2, if k is odd then every such p satisfies

$$\left(\frac{a_p(f_\alpha^k)}{p}\right) = 1, \tag{3.4}$$

while if k is even such a p satisfies (3.4) if and only if it splits completely in $\mathbf{Q}(\sqrt[4]{-d}, i)/\mathbf{Q}$. By the Cebatorev density theorem the set of such primes has density $\frac{1}{4}$ or $\frac{1}{8}$, respectively.

Next consider primes $p \equiv 3 \pmod 4$, p relatively prime to α and split in $K/\mathbf{Q}$. These primes are inert in $\mathbf{Q}(i)/\mathbf{Q}$, and by Proposition 3.2 they satisfy(3.4) if and only if they split in $\mathbf{Q}(\sqrt{\alpha})/\mathbf{Q}$. In particular, the set of such primes has density $\frac{1}{8}$ unless $\mathbf{Q}(\sqrt{\alpha})$ lies in $\mathbf{Q}(\sqrt{-d}, i)$. This occurs only if $D(\alpha) \in \{1, D\}$ or $D(\alpha') \in \{-4, 4d\}$, in which case these primes have density $\frac{1}{4}$ or 0, respectively. The proposition now follows easily in these cases. ∎

4 Higher powers

4.1 Cubes

For the field $K = \mathbf{Q}(\sqrt{-3})$ it is possible to use the law of cubic reciprocity to study the cubic character of the Fourier coefficients of the CM form f_α^k.

Proposition 4.1 *Assume $d = 3$. Fix $k \geq 2$ and $\alpha \in \mathbf{Q}^\times$. Let $p \equiv 1 \pmod 3$ be a rational prime, relatively prime to α, which splits in $K/\mathbf{Q}$. Then*

$$\left(\frac{a_p(f_\alpha^k)}{p}\right)_3 = \begin{cases} 1 & p \equiv 1 \pmod 9; \\ \left(\frac{\alpha}{p}\right)_3^2 & p \equiv 4 \pmod 9; \\ \left(\frac{\alpha}{p}\right)_3 & p \equiv 7 \pmod 9. \end{cases}$$

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

Proof Let π be a prime divisor of p which is congruent to 1 modulo 3. By the law of cubic reciprocity (see, for example, [7, Section 7.2]) we have

$$\left(\frac{\pi}{\bar{\pi}}\right)_3 = \left(\frac{\bar{\pi}}{\pi}\right)_3.$$

On the other hand,

$$\overline{\left(\frac{\pi}{\bar{\pi}}\right)_3} = \left(\frac{\bar{\pi}}{\pi}\right)_3;$$

it follows that in fact $\left(\frac{\pi}{\bar{\pi}}\right)_3 = 1$. In particular, by Lemma 2.5 and the definition of ψ_α^k we have

$$\left(\frac{a_p(f_\alpha^k)}{p}\right)_3 = \left(\frac{\pi}{\bar{\pi}}\right)_3^{k-1}\left(\frac{\left(\frac{-1}{p}\right)}{p}\right)_3^{k-1}\left(\frac{\left(\frac{\alpha}{p}\right)_6}{\bar{\pi}}\right)_3 = \left(\frac{\left(\frac{\alpha}{p}\right)_6}{\bar{\pi}}\right)_3$$
$$= \left(\frac{\alpha}{p}\right)_6^{(p-1)/3} = \left(\frac{\alpha}{p}\right)_3^{(p-1)/6};$$

the proposition follows easily. ∎

Theorem 4.2 *Assume $d = 3$. Fix $k \geq 2$ and $\alpha \in \mathbf{Q}^\times$. Then*

$$\delta_3(f_\alpha^k) = \begin{cases} 1 & \alpha \in \mathbf{Q}^{\times 3}; \\ 5/9 & \alpha \notin \mathbf{Q}^{\times 3}. \end{cases}$$

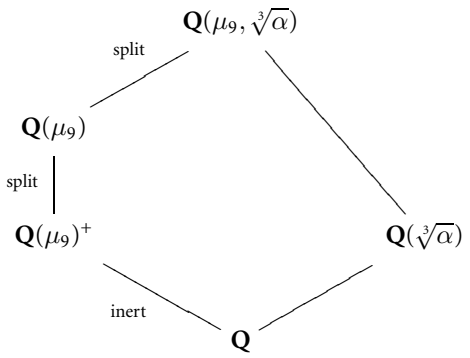
Proof If $\alpha \in \mathbf{Q}^{\times 3}$, then $\left(\frac{\alpha}{p}\right)_3 = 1$ for all $p \equiv 1 \pmod 3$, so that $\delta_3(f_\alpha^k) = 1$ by Proposition 4.1. On the other hand, if $\alpha \notin \mathbf{Q}^{\times 3}$, then primes $p \equiv 1 \pmod 9$ always satisfy

$$\left(\frac{a_p(\psi_\alpha^k)}{p}\right)_3 = 1, \tag{4.1}$$

while primes $p \equiv 4, 7 \pmod 9$ satisfy (4.1) if and only if $\left(\frac{\alpha}{p}\right)_3 = 1$. The former condition is equivalent to p splitting completely in $\mathbf{Q}(\mu_9)/\mathbf{Q}$, so that the set of such p has density $\frac{1}{6}$. The latter condition is equivalent to p having inertial degree 3 in $\mathbf{Q}(\mu_9)/\mathbf{Q}$ and splitting completely in $\mathbf{Q}(\mu_9, \sqrt[3]{\alpha})/\mathbf{Q}(\mu_9)$. The unique cubic subfield of $\mathbf{Q}(\mu_9)$ is $\mathbf{Q}(\mu_9)^+$, which is Galois over $\mathbf{Q}$ and thus can not contain any non-trivial cube roots. Thus $\mathbf{Q}(\mu_9) \cap \mathbf{Q}(\sqrt[3]{\alpha}) = \mathbf{Q}$, so that the set of such p has density $\frac{2}{3} \cdot \frac{1}{2} \cdot \frac{1}{3} = \frac{1}{9}$

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

by the Cebatorev theorem.



Combining these results, we see that the set of $p \equiv 1 \pmod 3$ with

$$\left(\frac{a_p(f_\alpha^k)}{p}\right)_3 = 1$$

has density $\frac{5}{18}$, from which it follows that $\delta_3(f_\alpha^k) = \frac{5}{9}$, as claimed. ∎

4.2 m-th Powers, $m \mid k-1$

For any $\alpha \in \mathbf{Q}^\times$ we write $D(\alpha)$ for the discriminant of the quadratic field $\mathbf{Q}(\sqrt{\alpha})$ over $\mathbf{Q}$. For simplicity we state the next result only for $d > 3$; the cases become overwhelming for $d \leq 3$.

Theorem 4.3 *Assume that $d > 3$ and fix $k \geq 2$, $k \equiv 1 \pmod h$, and $\alpha \in \mathbf{Q}^\times$. Then for any $m \mid k-1$ we have*

$$\delta_m(f_\alpha^k) = \begin{cases} 1 & m \text{ odd or } D(\alpha)|m \text{ or } D(-d\alpha)|m; \\ 1/2 & m \text{ even and } D(\alpha) \nmid m \text{ and } D(-d\alpha) \nmid m \text{ and either} \\ & D(\alpha)|2m \text{ or } D(-d\alpha)|2m; \\ 3/4 & \text{otherwise.} \end{cases}$$

Proof Let $p \equiv 1 \pmod m$ be a prime which splits as $\mathfrak{p}\bar{\mathfrak{p}}$ in $K/\mathbf{Q}$. By Lemma 2.5 and the definition of ψ_α^k we have

$$\left(\frac{a_p(f_\alpha^k)}{p}\right)_m = \left(\frac{\psi'^{k-1}(\mathfrak{P}) \cdot \left(\frac{\varepsilon}{p}\right)^{(k-1)/h} \cdot \left(\frac{\alpha}{p}\right)}{\bar{\mathfrak{p}}}\right)_m = \left(\frac{\left(\frac{\varepsilon}{p}\right)^{(k-1)/h} \cdot \left(\frac{\alpha}{p}\right)}{p}\right)_m$$

for any prime $\mathfrak{P}$ of H lying over $\mathfrak{p}$. Since h is odd and $\left(\frac{\varepsilon}{p}\right) = \pm 1$, we certainly have

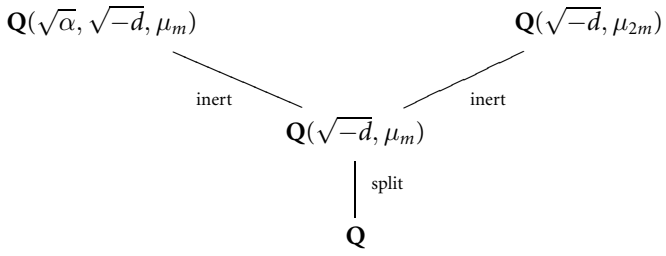
$$\left(\frac{\left(\frac{\varepsilon}{p}\right)}{p}\right)_m^{(k-1)/h} = 1,$$

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

so that

$$\left(\frac{a_p(f_\alpha^k)}{p}\right)_m = \left(\frac{\left(\frac{\alpha}{p}\right)}{p}\right)_m.$$

This is not equal to 1 if and only if both $\left(\frac{\alpha}{p}\right)$ and $\left(\frac{-1}{p}\right)_m$ equal -1. (Note that $\left(\frac{-1}{p}\right)_m = \pm 1$ since $p \equiv 1 \pmod{m}$.) This in turn is equivalent to the following splitting behavior of p:



In particular, there are no such primes (so that $\delta_m(f_\alpha^k) = 1$) if and only if either of the top two extensions are trivial. If both of these extensions are non-trivial, then it follows from the Cebatorev theorem that $\delta_m(f_\alpha^k) = \frac{3}{4}$ unless the two extensions coincide, in which case $\delta_m(f_\alpha^k) = \frac{1}{2}$. One now checks easily using Lemma 4.4 below (and the fact that $\mathbf{Q}(\mu_m) = \mathbf{Q}(\mu_{2m})$ if and only if m is odd) that the conditions given in the statement of the theorem are equivalent to these field theoretic conditions. ■

We remark that this result recovers Theorem 3.3 when k is odd.

Lemma 4.4 *Fix $n \geq 1$ and $\alpha, \beta \in \mathbf{Q}^\times$. Then*

$$[\mathbf{Q}(\sqrt{\alpha}, \sqrt{\beta}, \mu_n) : \mathbf{Q}] = \begin{cases} \varphi(n) & D(\alpha) \text{ and } D(\beta) \text{ divide } n; \\ 2\varphi(n) & \text{exactly one of } D(\alpha), D(\beta), D(\alpha\beta) \text{ divides } n; \\ 4\varphi(n) & \text{otherwise.} \end{cases}$$

Proof Set $F = \mathbf{Q}(\sqrt{\alpha}, \sqrt{\beta})$. We have

$$[F(\mu_n) : \mathbf{Q}] = [F : F \cap \mathbf{Q}(\mu_n)] \cdot [\mathbf{Q}(\mu_n) : \mathbf{Q}] = [F : F \cap \mathbf{Q}(\mu_n)] \cdot \varphi(n).$$

Note that $\mathbf{Q}(\mu_{D(\alpha)})$ is the smallest cyclotomic field containing $\sqrt{\alpha}$, so that in general $\sqrt{\alpha} \in \mathbf{Q}(\mu_n)$ if and only if $D(\alpha)$ divides n. As every subfield of F is generated by some subset of $\{\sqrt{\alpha}, \sqrt{\beta}, \sqrt{\alpha\beta}\}$, this allows one to easily compute $F \cap \mathbf{Q}(\mu_n)$ in terms of $D(\alpha)$, $D(\beta)$, and $D(\alpha\beta)$. The lemma follows from this computation. ■

Acknowledgements It is a pleasure to thank Ravi Ramakrishna for suggesting this problem and for all of the encouragement and insight he provided. I would also like to thank Rob Benedetto, Ken Ribet, and Siman Wong for helpful conversations and the referee for many useful corrections.

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press

References

[1] J. Cremona, *Algorithms for Modular Elliptic Curves.* Second edition, Cambridge University Press, Cambridge, 1997.

[2] P. Deligne, *La conjecture de Weil. I.* Inst. Hautes Études Sci. Publ. Math. **43**(1974), 273–307.

[3] E. de Shalit, *Iwasawa theory of elliptic curves with complex multiplication. p-adic L functions.* Perspectives in Mathematics 3, Academic Press, Boston, MA, 1987.

[4] J.-M. Fontaine and B. Mazur, *Geometric Galois representations.* In: Elliptic Curves, Modular Forms and Fermat's Last Theorem, Number Theory 1, International Press, Cambridge, MA, 1995, pp. 41–78.

[5] B. Gross, *Arithmetic on elliptic curves with complex multiplication.* Lecture Notes in Mathematics 776, Springer-Verlag, Berlin, 1980.

[6] C. Khare, M.l Larsen, and R. Ramakrishna, *Construction of semisimple p-adic Galois representations with prescribed properties*, preprint.

[7] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein.* Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[8] K. Ribet, *Galois representations attached to eigenforms with nebentypus.* In: Modular Functions of One Variable, V, Lectures Notes in Math. 601, Springer, Berlin, 1977, pp. 7–51.

[9] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer.* In: Arithmetic Theory of Elliptic Curves, Lectures Notes in Math. 1716, Springer, Berlin, 1999, pp. 167–234.

[10] A. Scholl, *Motives for modular forms*, Invent. Math. **100**(1990), 419–430.

[11] J. Silverman, *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics 151, Springer-Verlag, New York, 1994.

[12] William Stein, *The modular forms explorer*, available at: http://modular.fas.harvard.edu/mfd/mfe/.

Department of Mathematics and Statistics
University of Massachusetts, Amherst
Amherst, MA 01003
U.S.A.
e-mail: weston@math.umass.edu

https://doi.org/10.4153/CJM-2005-042-5 Published online by Cambridge University Press