



HAL
open science

CLASS NUMBER FORMULAS FOR CERTAIN BIQUADRATIC FIELDS

Elizabeth Athaide, Emma Cardwell, Christy Thompson

► **To cite this version:**

Elizabeth Athaide, Emma Cardwell, Christy Thompson. CLASS NUMBER FORMULAS FOR CERTAIN BIQUADRATIC FIELDS. Hardy-Ramanujan Journal, 2023, 46, pp.63 – 89. 10.46298/hrj.2024.12573 . hal-04292835v2

HAL Id: hal-04292835

<https://hal.science/hal-04292835v2>

Submitted on 27 Feb 2024 (v2), last revised 28 Feb 2024 (v3)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial 4.0 International License

Class Number Formulas for Certain Biquadratic Fields

Elizabeth Athaide, Emma Cardwell and Christina Thompson

Abstract. We consider the class numbers of imaginary quadratic extensions $F(\sqrt{-p})$, for certain primes p , of totally real quadratic fields F which have class number one. Using seminal work of Shintani, we obtain two elementary class number formulas for many such fields. The first expresses the class number as an alternating sum of terms that we generate from the coefficients of the power series expansions of two simple rational functions that depend on the arithmetic of F and p . The second makes use of expansions of $1/p$, where p is a prime such that $p \equiv 3 \pmod{4}$ and p remains inert in F . More precisely, for a generator ε_F of the totally positive unit group of \mathcal{O}_F , the base- ε_F expansion of $1/p$ has period length $\ell_{F,p}$, and our second class number formula expresses the class number as a finite sum over disjoint cosets of size $\ell_{F,p}$.

Keywords. class numbers of imaginary quadratic extensions, Shintani sets, Shintani cycles, Hecke character.

2010 Mathematics Subject Classification. 11R29

1. Introduction

The theory of class numbers has a rich history, beginning with Gauss's effort to understand how primes could be represented by positive definite binary quadratic forms [Cox89]. Gauss recognized that $\mathrm{SL}_2(\mathbb{Z})$ acts naturally on positive definite integral binary quadratic forms $f(X, Y) = aX^2 + bXY + cY^2$ with fixed discriminant $-d = b^2 - 4ac$. He proved that the set of equivalence classes under this action is a finite abelian group; the order of this group is known as the *class number* $h(-d)$. The class group for quadratic forms of discriminant d is also isomorphic to the ideal class group for the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{d})$. Therefore, it is natural to ask whether results about Gauss's class numbers are glimpses of results for the class numbers h_K of more general number fields K . In this spirit, we recall two surprising results for Gauss's class numbers.

In the 1970s, Hirzebruch [Hir87] and Zagier [Zag75] found an elegant formula for $h(-p)$, when $7 \leq p \equiv 3 \pmod{4}$ is prime and $h(4p) = 1$. If the simple continued fraction for \sqrt{p} is written as

$$\sqrt{p} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots}}}} = [a_0, \overline{a_1, \dots, a_{2t}}],$$

where the repeating period begins with a_1 and has minimal even length $2t$, they proved that

$$h(-p) = \frac{1}{3} \sum_{k=1}^{2t} (-1)^k a_k. \quad (1.1)$$

More recently in the 1990s, Girstmair [Gir94] found another elegant formula as an alternating sum of numbers that are even simpler to describe. Namely, if g is a primitive root modulo p , he examines the base g expansion of $1/p$, which is eventually periodic with period length $p-1$ (see [HaWr2008], Section 9.6). If this period is $\overline{x_1 x_2 \dots x_{p-1}}$, where $0 \leq x_i \leq g-1$, then he proved that

$$h(-p) = \frac{1}{g+1} \sum_{k=1}^{p-1} (-1)^k x_k. \quad (1.2)$$

A priori, these results are unexpected relationships between combinatorial sums and class numbers of binary quadratic forms with discriminant $-p$. Since class numbers of binary quadratic forms are also examples of class numbers of number fields, it is natural to ask whether (1.1) and (1.2) are glimpses of a more general theory where class numbers of number fields can be described as alternating sums of combinatorial numbers. We show that this is indeed the case for a large class of imaginary quadratic extensions of real quadratic fields F . To make this precise, suppose that $F = \mathbb{Q}(\sqrt{d})$, where $d > 1$ is square-free. Throughout, we assume that its ring of integers \mathcal{O}_F has class number 1. We note that $\mathcal{O}_F = \mathbb{Z}[\theta_F]$, where we let

$$\theta_F := \begin{cases} \sqrt{d} & \text{if } d \equiv 3 \pmod{4} \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

The imaginary quadratic extensions of F that we consider are of the form $F(\sqrt{-p})$, where p is a prime for which $7 \leq p \equiv 3 \pmod{4}$ and $\left(\frac{d}{p}\right) = -1$. These conditions imply that the relative discriminant ideal is the prime ideal $p\mathcal{O}_F$ (see Lemma 2.3). Moreover, for convenience, we fix a generator $\rho_{F,p} := a + b\theta_F \in \mathcal{O}_F$ such that $(\mathcal{O}_F/p\mathcal{O}_F)^\times = \langle \rho_{F,p} + p\mathcal{O}_F \rangle \cong \mathbb{F}_{p^2}^\times$.

In this setting, we derive a class number formula for $F(\sqrt{-p})$ as an alternating sum that arises from p and invariants of F . Our key observation is that the combinatorial structure that underlies (1.1) and (1.2) can be reformulated in terms of recurrence relations that can be captured by the coefficients of distinguished rational functions. Therefore, our goal is to define two rational functions (reflecting that F has degree 2 over \mathbb{Q}) whose coefficients can be incorporated into an alternating sum that yields the class number $h_{F(\sqrt{-p})}$.

To this end, we use $\rho_{F,p} = a + b\theta_F$ to define integers

$$C_{F,p} := a^2 + ab \cdot \text{Tr}_{F/\mathbb{Q}}(\theta_F) + \text{Norm}_{F/\mathbb{Q}}(\theta_F)b^2, \quad (1.3)$$

$$D_{F,p} := 2a + b \cdot \text{Tr}_{F/\mathbb{Q}}(\theta_F), \quad (1.4)$$

and in turn, to define the rational functions as

$$X_{F,p}(z) = \sum_{m \geq 1} x(m)z^m := \frac{az - C_{F,p}z^2}{C_{F,p}z^2 - D_{F,p}z + 1}, \quad (1.5)$$

$$Y_{F,p}(z) = \sum_{m \geq 1} y(m)z^m := \frac{bz}{C_{F,p}z^2 - D_{F,p}z + 1}. \quad (1.6)$$

Moreover, we must delicately take into account the presence of nontrivial units as they inform class number calculations. To make this precise, we recall that Dirichlet's Unit Theorem implies that $\mathcal{O}_F^\times = \{\pm \varepsilon_F^j, j \in \mathbb{Z}\}$, where $\varepsilon_F = s + t\theta_F$ is the totally positive fundamental unit. We then define t pairs of sequences, say $\{(x_i(m), y_i(m)) : m \geq 1\}$, where t is the coefficient of θ_F in ε_F , that encode the action of ε_F by means of expressions involving $x(m)$ and $y(m)$ (see (3.13)). Finally, we find that the analogues of the right hand side of (1.2) turn out to be obtained from the quadratic form

$$Q_F(Y_1, Y_2) := \text{Tr}_{F/\mathbb{Q}}(\varepsilon_F)Y_1^2 + 4Y_1Y_2 + \text{Tr}_{F/\mathbb{Q}}(\varepsilon_F)Y_2^2.$$

In terms of this data, we obtain the following theorem, which gives a formula for the class number $h_{F(\sqrt{-p})}$.

Theorem 1.1. *Assuming the notation and hypotheses above, we have*

$$h_{F(\sqrt{-p})} = \frac{1}{16t^2p^2} \sum_{\substack{1 \leq m \leq p^2-1 \\ 1 \leq i \leq t}} (-1)^m Q_F(x_i(m), y_i(m)).$$

Remark. For real quadratic fields F with $h_F = 1$, Theorem 1.1 applies for one-fourth of the primes. This follows from the strong version of Dirichlet’s Theorem on primes in arithmetic progressions, which implies that the primes p such that $p \equiv 3 \pmod{4}$ and $\left(\frac{d}{p}\right) = -1$ have density $1/4$.

Example. Here we illustrate Theorem 1.1 with $F = \mathbb{Q}(\sqrt{3})$ and $p = 7$. The field $F(\sqrt{-7})$ has class number $h_{F(\sqrt{-7})} = 2$. Note that F has class number 1, and its totally positive fundamental unit is $\varepsilon_F = 2 + \sqrt{3}$, and so $t = 1$. The prime $p = 7$ satisfies the required conditions that $p \equiv 3 \pmod{4}$ and $\left(\frac{3}{7}\right) = -1$. Therefore, we have that the principal ideal $7\mathcal{O}_F \subset \mathcal{O}_F = \mathbb{Z}[\sqrt{3}]$ is prime, and so we have that $\mathcal{O}_F/7\mathcal{O}_F \cong \mathbb{F}_{49}$. One can check that $\rho_{F,p} = 6 + \sqrt{3}$ generates the multiplicative cyclic group $(\mathcal{O}_F/7\mathcal{O}_F)^\times \cong \mathbb{F}_{49}^\times$. Thus we have $a = 6, b = 1$, and using (1.3) and (1.4), we find that $C_{F,p} = 33$, and $D_{F,p} = -12$, which in turn by (1.5) and (1.6) give

$$X_{F,p}(z) = \sum_{m \geq 1} x(m)z^m = 6z + 39z^2 + 270z^3 + 1953z^4 + \dots = \frac{6z - 33z^2}{33z^2 + 12z + 1},$$

$$Y_{F,p}(z) = \sum_{m \geq 1} y(m)z^m = z + 12z^2 + 111z^3 + 936z^4 + \dots = \frac{z}{33z^2 + 12z + 1}.$$

Theorem 1.1 offers a formula for $h_{F(\sqrt{-7})}$ as an alternating sum of $7^2 - 1 = 48$ terms that are assembled from the first 48 coefficients of $X_{F,p}(z)$ and $Y_{F,p}(z)$. Furthermore, because $t = 1$, the relevant pairs $\{x_1(m), y_1(m)\}$ are merely reductions of the pairs of coefficients $\{x(m), y(m)\}$ to a specific *fundamental domain*, as given in (3.13). One finds that

$$\begin{aligned} x_1(1) &= 1, & x_1(2) &= -5, & \dots, & x_1(48) &= -5, \\ y_1(1) &= -5, & y_1(2) &= -4, & \dots, & y_1(48) &= -7. \end{aligned}$$

We now use Theorem 1.1 to calculate $h_{F(\sqrt{-7})}$:

$$\begin{aligned} h_{F(\sqrt{-7})} &= \frac{1}{784} \sum_{1 \leq m \leq 48} (-1)^m \left[4x_1(m)^2 + 4x_1(m)y_1(m) + 4y_1(m)^2 \right] \\ &= \frac{1}{784} (-84 + 76 - 300 + 52 - 28 + \dots + 436) = 2. \end{aligned}$$

We circle back to the fact that the class number formula in (1.2) makes use of the base g expansion of $1/p$. We stress that the number of terms in the sum, which is $p - 1$, is the length of the repeating period of this expansion. Therefore, we ask whether the expression in Theorem 1.1 can be reformulated so that the number of terms in the sum equals the period length of an analogous expansion of $1/p$. We find, indeed, that this is the case.

In the setting of Theorem 1.1, it is natural to consider the *base- ε_F expansion* of elements $\alpha \in F$. To be precise, there is a unique sequence of integers $a_n, a_{n-1}, \dots, a_0, a_{-1}, a_{-2}, \dots$, with $0 \leq a_i \leq \lfloor \varepsilon_F \rfloor$, for which

$$\alpha = a_n \varepsilon_F^n + a_{n-1} \varepsilon_F^{n-1} + \dots + a_0 + a_{-1} \varepsilon_F^{-1} + a_{-2} \varepsilon_F^{-2} + \dots \tag{1.7}$$

The above expression is called the *base- ε_F expansion* of α , and it is well-known that such expansions are eventually periodic (see, for example, [Sch80]). To recast Theorem 1.1 in terms of these expansions, we require the following finite set:

$$R_{F,p} := \left\{ r_1 + r_2 \varepsilon_F \in \frac{1}{p} \mathcal{O}_F : r_1 \in \mathbb{Q} \cap (0, 1], r_2 \in \mathbb{Q} \cap [0, 1) \right\}, \tag{1.8}$$

which is known as the *Shintani set* for F at p , when $p \equiv 3 \pmod{4}$ and $\left(\frac{d}{p}\right) = -1$. The totally positive units define a group action of $\mathcal{O}_F^{\times,+} := \langle \varepsilon_F \rangle$ onto $R_{F,p}$ as follows.

$$\varepsilon_F * (r_1 + r_2 \varepsilon_F) := (1 - r_2) + \{r_1 + r_2 \operatorname{Tr}_{F/\mathbb{Q}}(\varepsilon_F)\} \varepsilon_F,$$

where $\{x\} := x - \lfloor x \rfloor$ is the fractional part of x . Under this action, the set $R_{F,p}$ is a finite disjoint union of orbits, say

$$R_{F,p} = \bigsqcup_{r \in \mathcal{O}_F^{\times,+} \setminus R_{F,p}} \mathcal{O}_F^{\times,+} * r.$$

For $r \in R_{F,p} \setminus \mathcal{O}_F$, we prove (see Lemma 4.8) that the number of elements in the orbit of r under ε_F is equal to the period length of $1/p$ in base ε_F , which we denote $\ell_{F,p}$. This allows us to now state the desired class number formula as a sum over $\ell_{F,p}$ terms, where we make the following abuse of notation:

$$Q_F(r_1 + r_2 \varepsilon_F) = Q_F(r_1, r_2).$$

Theorem 1.2. *Assuming the notation and hypotheses from Theorem 1.1, we have*

$$h_{F(\sqrt{-p})} = \frac{1}{4} \sum_{i=1}^{\ell_{F,p}} \sum_{r \in \mathcal{O}_F^{\times,+} \setminus R_{F,p}} \chi_{F(\sqrt{-p})/F}(rp\mathcal{O}_F) Q_F(\varepsilon_F^i * r),$$

where $\chi_{F(\sqrt{-p})/F}$ is the unique quadratic Hecke character of conductor $p\mathcal{O}_F$.

Example. Now we illustrate Theorem 1.2 with $F = \mathbb{Q}(\sqrt{3})$ and $p = 7$, where $h_F = 1$ and $\varepsilon_F = 2 + \sqrt{3}$ (so $t = 1$). One can check (for example, using SageMath) that the base- ε_F expansion of $1/7$ is

$$\begin{aligned} \frac{1}{7} &= \varepsilon_F^{-2} + \sum_{i=0}^{\infty} (3\varepsilon_F^{-8i-3} + 2\varepsilon_F^{-8i-4} + 2\varepsilon_F^{-8i-5} + 2\varepsilon_F^{-8i-7} + 2\varepsilon_F^{-8i-8} + 3\varepsilon_F^{-8i-9}) \\ &= 0.01\overline{32202230}. \end{aligned}$$

Thus, we see that the base ε_F expansion of $1/7$ has period length $\ell_{F,7} = 8$. Since $|R_{F,7} - \mathcal{O}_F| = tp^2 - t = 48$ (see Lemmas 2.6 and 2.9), we deduce that $\mathcal{O}_F^{\times,+} \setminus (R_{F,7} - \mathcal{O}_F)$ contains $48/\ell_{F,7} = 6$ disjoint orbits. One can also verify that the set

$$\left\{ \frac{1}{7} + \frac{1}{7}\varepsilon_F, \frac{1}{7}, \frac{1}{7} + \frac{4}{7}\varepsilon_F, \frac{1}{7} + \frac{5}{7}\varepsilon_F, \frac{2}{7} + \frac{2}{7}\varepsilon_F, \frac{3}{7} \right\}.$$

is a complete set of orbit representatives for $\mathcal{O}_F^{\times,+} \setminus (R_{F,7} - \mathcal{O}_F)$. Equipped with these values, Theorem 1.2 states that

$$\begin{aligned} h_{F(\sqrt{-7})} &= \frac{1}{4} \sum_{i=1}^8 \sum_{r \in R_{F,p} \setminus \mathcal{O}_F^{\times,+}} \chi_{F(\sqrt{-7})/F}(rp\mathcal{O}_F) Q_F(\varepsilon_F^i * r) \\ &= \frac{1}{4} \left(-\frac{220}{7} + \frac{228}{7} - \frac{188}{7} + \frac{212}{7} - \frac{180}{7} + \frac{204}{7} \right) = 2. \end{aligned}$$

Remark. We do not believe that these results will be useful for improving the efficiency of algorithms that compute class numbers.

Theorems 1.1 and 1.2 are generalizations of the results from Hirzebruch-Zagier and Girstmair to the setting of imaginary quadratic extensions of real quadratic fields F with $h_F = 1$. Within this new setting, we prove our theorems by working with a class number formula analogous to the one used in the quadratic setting by Hirzebruch, Zagier, and Girstmair.

Both (1.1) and (1.2) arise from a finite version of Dirichlet's class number formula, which relates the Dirichlet L -function, an infinite series, to the class number of $\mathbb{Q}(\sqrt{-d})$:

$$L(1, \chi_d) = \frac{2\pi}{\omega\sqrt{d}} h(-d),$$

where ω represents the number of roots of unity in $\mathbb{Q}(\sqrt{-d})$, and χ_d is a primitive Dirichlet character of conductor d . Using the functional equation of this L -function, the above equation can be written in terms of $L(0, \chi_d)$, which in turn allows us to use the Hurwitz ζ -function and the periodicity of χ_d to rewrite this class number formula as a finite sum of Bernoulli polynomials evaluated at integer points. Our work uses an analogous formula of Shintani [Shi76], which expresses the class numbers of totally imaginary quadratic extensions of totally real fields as finite sums assembled from Bernoulli numbers.

In Section 2, we review the background needed to state Shintani's class number formula for imaginary quadratic extensions of real quadratic fields F with $h_F = 1$. These formulae involve "Shintani sets," which are something like fundamental domains for the action of the totally positive units on $\frac{1}{p}\mathcal{O}_F$. The crux of our work relies on combinatorial properties of these sets, which we derive in Section 2. Then, we prove Theorem 1.1 in Section 3 and Theorem 1.2 in Section 4. Finally, in Section 5, we use Theorems 1.1 and 1.2 to calculate class numbers of $\mathbb{Q}(\sqrt{3}, \sqrt{-p})$, where $p \equiv 3 \pmod{4}$ is prime, $\left(\frac{d}{p}\right) = -1$, and $p < 100$.

2. Shintani's Class Number Formula and Properties of Shintani Sets

In this section, we discuss the background needed to state Shintani's class number formula. While Shintani's theorem is true for totally imaginary quadratic extensions of a totally real field of arbitrary degree, we restrict the following commentary and definitions to the case that F is quadratic with class number 1. Throughout this section, we fix a real quadratic field F of class number 1 and a totally imaginary quadratic extension of F , which we denote $K = F(\sqrt{-p})$, where $p \equiv 3 \pmod{4}$.

2.A. Algebraic Background

Shintani's formula can be used to calculate the relative class number h_K/h_F in terms of invariants of F , K , and the extension K/F itself. Before stating the formula, we review the definitions of these invariants.

The *regulator* R_L of a number field L measures the density of units in the ring of integers. The regulator can be determined by considering the matrix

$$[N_j \log(\sigma_j(u_i))],$$

where each u_i is a fundamental unit from the set u_1, \dots, u_k generating the unit group in \mathcal{O}_L , each σ_j is a unique Archimedean place of L , and N_j is defined to be 1 if σ_j is real, and 2 if σ_j is complex. If we define r_1 and r_2 respectively to be the number of real and complex embeddings of L , by Dirichlet's unit theorem, we see that this matrix has dimension $(r_1 + r_2 - 1) \times (r_1 + r_2)$. The regulator R_L is the determinant of the square submatrix which is formed by deleting any single column of this matrix. Since the sum of the entries in each row of this matrix is 0, this determinant is independent of which column is deleted. If we consider the rows of this matrix as forming a lattice in $\mathbb{R}^{r_1+r_2-1}$, then the regulator is directly proportional to the volume of the fundamental domain associated to this lattice.

Next, we examine the unit groups of \mathcal{O}_K and \mathcal{O}_F . Since F is a real quadratic field, and K is a totally imaginary quadratic extension of F , Dirichlet's unit theorem implies that \mathcal{O}_F and \mathcal{O}_K are both \mathbb{Z} -modules of rank 1. More precisely, if we let μ_F and μ_K represent the groups of roots of unity in F and K respectively, there exists $\varepsilon_F \in \mathcal{O}_F$ and $\varepsilon_K \in \mathcal{O}_K$ such that $\mathcal{O}_F^\times = \mu_F \times \langle \varepsilon_F \rangle$ and $\mathcal{O}_K^\times = \mu_K \times \langle \varepsilon_K \rangle$. Since F is real quadratic and any of $\varepsilon_F, -\varepsilon_F, \varepsilon_F^{-1}, -\varepsilon_F^{-1}$ can generate the free part of \mathcal{O}_F , we can choose ε_F to be totally positive and greater than 1.

Lemma 2.1. *We have $\mathcal{O}_K^\times = \mathcal{O}_F^\times$. In particular, we may choose $\varepsilon_K = \varepsilon_F$.*

Proof. A theorem by Fröhlich and Taylor shows that $[\mathcal{O}_K^\times : \mathcal{O}_F^\times \mu_K] = 1$ or 2 (see Theorem 42 in [FrTa91]). Since $K = \mathbb{Q}(\sqrt{d}, \sqrt{-p})$ for $p \geq 7$, $\mu_K = \{\pm 1\}$. Thus $\mu_K = \mu_F$, so $[\mathcal{O}_K^\times : \mathcal{O}_F^\times] = 1$ or 2 .

Now, assume for the sake of contradiction that $[\mathcal{O}_K^\times : \mathcal{O}_F^\times] = 2$, so $\varepsilon_K \notin \mathcal{O}_F^\times$, and $\varepsilon_K^2 \in \mathcal{O}_F^\times$. Since $K \cap \mathbb{R} = F$, we see that $\varepsilon_K \notin \mathbb{R}$. However, we know that $\varepsilon_K^2 \in \mathcal{O}_F \subset \mathbb{R}$. Observe that both $\varepsilon_K \in \mathbb{C} - \mathbb{R}$ and $\varepsilon_K^2 \in \mathbb{R}$ if and only if $\operatorname{Re}(\varepsilon_K) = 0$. Additionally, $\operatorname{Norm}_{K/\mathbb{Q}}(\varepsilon_K) = \pm 1$, which implies that $\varepsilon_K = \pm i$. However, this is a contradiction since $\pm i \notin K$, so we see that $[\mathcal{O}_K^\times : \mathcal{O}_F^\times] = 1$, and hence $\mathcal{O}_K^\times = \mu_F \times \langle \varepsilon_F \rangle = \mu_K \times \langle \varepsilon_F \rangle$, so we can choose $\varepsilon_K = \varepsilon_F$. \square

Equipped with the fact that $\varepsilon_K = \varepsilon_F$, we may now relate the regulators R_K and R_F of K and F , which we do in the lemma which follows.

Lemma 2.2. *For F and K as defined in the beginning of this section, we have that $R_K = 2R_F$.*

Proof. Since $\varepsilon_F = \varepsilon_K$ by Lemma 2.1, the regulators of the fields F and K as previously defined are determined using the following matrices:

$$\begin{aligned} R_F &: [\log |\varepsilon_F| & \log |-\varepsilon_F|] \\ R_K &: [2 \log |\varepsilon_F| & 2 \log |-\varepsilon_F|] \end{aligned}$$

Thus $R_F = \log |\varepsilon_F|$ and $R_K = 2 \log |\varepsilon_F| = 2R_F$. \square

Next, we review the definition of the *relative discriminant ideal* $D_{K/F}$ for our fields K and F . Recall that F has class number 1, so $D_{K/F}$ is principal. Since K/F is quadratic, it is Galois, and its Galois group consists of two elements: the identity and complex conjugation. In this setting, $D_{K/F}$ is given by

$$D_{K/F} := \left(\det \begin{bmatrix} \omega_1 & \omega_2 \\ \bar{\omega}_1 & \bar{\omega}_2 \end{bmatrix} \right)^2 \mathcal{O}_F,$$

where $\{\omega_1, \omega_2\}$ is an integral basis of K/F . We know that an integral basis will exist in our case by the following argument. From the structure theorem for finitely generated modules over a Dedekind domain, we have that $\mathcal{O}_K \cong \mathcal{O}_F^n \oplus \mathfrak{a}$, where \mathfrak{a} is an ideal of \mathcal{O}_F and $n \in \mathbb{Z}_{\geq 0}$ (see Theorem 1.32 of [Nar90]). Since $h_F = 1$, implying \mathcal{O}_F is a principal ideal domain, \mathcal{O}_K must be a free \mathcal{O}_F -module of rank $2 = [K : F]$.

Lemma 2.3. *The set $\{1, \frac{1+\sqrt{-p}}{2}\}$ is an integral basis of K/F , and thus we have $D_{K/F} = p\mathcal{O}_F$.*

Proof. Let A be the change-of-basis matrix from the integral basis $\{\omega_1, \omega_2\}$ to the F -basis $\{1, \frac{1+\sqrt{-p}}{2}\}$. We see that

$$p\mathcal{O}_F = \left(\det \begin{bmatrix} 1 & \frac{1+\sqrt{-p}}{2} \\ 1 & \frac{1-\sqrt{-p}}{2} \end{bmatrix} \right)^2 \mathcal{O}_F = (\det A)^2 D_{K/F}.$$

Since \mathcal{O}_F is a Dedekind domain, ideals in \mathcal{O}_F factor uniquely. Therefore since $p\mathcal{O}_F$ is prime by assumption, $\det A$ must be a unit in \mathcal{O}_F , so $A \in \text{GL}_2(\mathcal{O}_F)$. Thus, $\{1, \frac{1+\sqrt{-p}}{2}\}$ is an integral basis of K/F . Using this integral basis, we see that

$$D_{K/F} = \left(\frac{1 - \sqrt{-p}}{2} - \frac{1 + \sqrt{-p}}{2} \right)^2 \mathcal{O}_F = p\mathcal{O}_F.$$

□

Finally, since $\text{Gal}(K/F) \cong \mathbb{Z}/2\mathbb{Z}$, there is a unique nontrivial character $\chi : \text{Gal}(K/F) \rightarrow \mathbb{C}^\times$. By class field theory, we can consider the precomposition of χ with the Artin symbol to obtain a character $\chi_{K/F}$ of the group of fractional ideals that are relatively prime to $D_{K/F}$. This is known as the *Hecke character of K/F with conductor $D_{K/F}$* . By definition of the Artin symbol (see, for example, [Cox89] page 106), we can explicitly compute the value of $\chi_{K/F}$ for any prime ideal \mathfrak{p} :

$$\chi_{K/F}(\mathfrak{p}) = \begin{cases} 1 & \mathfrak{p} \text{ splits in } \mathcal{O}_K \\ -1 & \mathfrak{p} \text{ remains inert in } \mathcal{O}_K \\ 0 & \mathfrak{p} \text{ ramifies in } \mathcal{O}_K. \end{cases}$$

Remark. Shintani’s class number formula relies on the narrow ideal class group character with conductor $D_{K/F}$ evaluated at fractional ideals. This corresponds to a primitive Grössencharakter with modulus $D_{K/F}$ (see Prop. 6.9 in [Neu11]). Since $\text{Gal}(K/F) \cong \mathbb{Z}/2\mathbb{Z}$, the nontrivial character $\chi : \text{Gal}(K/F) \rightarrow \mathbb{C}^\times$ is unique and injective, so class field theory implies that the primitive Grössencharakter with modulus $D_{K/F}$ is unique and corresponds to χ . Hence, we can see that the character used in Shintani’s formula is exactly the Grössencharakter. For more details, see Sections 6 and 10 in [Neu11].

Remark. For any unit $u \in K$ and any ideal $\mathfrak{a} \subset \mathcal{O}_K$, $u \cdot \mathfrak{a} = \mathfrak{a}$, and hence $\chi_{K/F}(u \cdot \mathfrak{a}) = \chi_{K/F}(\mathfrak{a})$.

2.B. Shintani’s Class Number Formula

In this section, we prove a simplified version of Shintani’s formula for real quadratic base fields F with $h_F = 1$.

Proposition 2.4. *For a totally real quadratic extension F of \mathbb{Q} with $h_F = 1$ and $K = F(\sqrt{-p})$ a totally imaginary quadratic extension of F where $7 \leq p \equiv 3 \pmod{4}$ remains inert in \mathcal{O}_F , Shintani’s formula simplifies to the following:*

$$h_K = \frac{1}{2} \sum_{r \in R_{F,p}} \chi_{K/F} \left((r_1 + r_2 \varepsilon_F) D_{K/F} \right) \sum_{\substack{0 \leq l_1, l_2 \leq 2 \\ l_1 + l_2 = 2}} \frac{B_{l_1}(r_1)}{l_1!} \frac{B_{l_2}(r_2)}{l_2!} \text{Tr}_{F/\mathbb{Q}}(\varepsilon_F)^{l_2-1},$$

where

$$R_{F,p} = \left\{ r = r_1 + r_2 \varepsilon_F : 0 < r_1 \leq 1, 0 \leq r_2 < 1, r \in \frac{1}{p} \mathcal{O}_F \right\},$$

and $B_n(x)$ is the degree n Bernoulli polynomial. As $[F : \mathbb{Q}] = 2$, Shintani’s formula only requires the following Bernoulli polynomials:

$$B_0(x) = 1, \quad B_1(x) = x - \frac{1}{2}, \quad B_2(x) = x^2 - x + \frac{1}{6}.$$

Proof. We follow [Shi76] by first considering the embedding $F \rightarrow \mathbb{R}^2$ via

$$F \hookrightarrow \mathbb{R}^2 \quad \alpha \mapsto (\alpha, \alpha'),$$

where $\alpha \mapsto \alpha'$ is the nontrivial automorphism in $\text{Gal}(F/\mathbb{Q})$. Shintani shows that the first quadrant $\mathbb{R}_+^2 := \{(x, y) \in \mathbb{R}^2 : x, y > 0\}$ can be decomposed as the following disjoint union:

$$\mathbb{R}_+^2 = \bigcup_{\eta \in \mathcal{O}_F^{\times,+}} \eta C_1 \sqcup \bigcup_{\eta \in \mathcal{O}_F^{\times,+}} \eta C_2$$

where C_1 is generated by the images of $1, \varepsilon_F$ in \mathbb{R}^2 and C_2 is generated by the image of 1:

$$C_1 = \{\lambda_1(1, 1) + \lambda_2(\varepsilon_F, \varepsilon'_F) \in \mathbb{R}^2 : \lambda_1, \lambda_2 > 0\}, \quad C_2 = \{\lambda(1, 1) \in \mathbb{R}^2 : \lambda > 0\},$$

and $\eta \in \mathcal{O}_F^{\times,+}$ acts by component-wise multiplication. Next, for each cone C_i , Shintani defines the set $R(i, \frac{1}{p}\mathcal{O}_F)$ as the following vectors with components in $\mathbb{Q} \cap (0, 1]$:

$$\begin{aligned} R\left(1, \frac{1}{p}\mathcal{O}_F\right) &:= \left\{ (r_1, r_2) \in \mathbb{Q}^2 : 0 < r_1, r_2 \leq 1, r_1 + r_2\varepsilon_F \in \frac{1}{p}\mathcal{O}_F \right\} \\ R\left(2, \frac{1}{p}\mathcal{O}_F\right) &:= \left\{ r_3 \in \mathbb{Q} : 0 < r_3 \leq 1, r_3 \in \frac{1}{p}\mathcal{O}_F \right\}. \end{aligned}$$

Let $\chi_{K/F}$ be the unique quadratic character of the narrow ideal class group of F with conductor $p\mathcal{O}_F$, associated to K . Then, assuming the notation above, we have the class number formula

$$h_K = \frac{2\omega_K R_F}{R_K \left[\mathcal{O}_F^\times : \mathcal{O}_F^{\times,+} \right]} \left(\sum_{r \in R\left(1, \frac{1}{p}\mathcal{O}_F\right)} \chi_{K/F}\left((r_1 + r_2\varepsilon_F)p\mathcal{O}_F\right) \sum_{\substack{(l_1, l_2) \in \mathbb{Z}_{\geq 0}^2 \\ l_1 + l_2 = 2}} \frac{B_{l_1}(r_1)B_{l_2}(r_2)}{2 \cdot l_1!l_2!} \text{Tr}_{F/\mathbb{Q}}\left(\varepsilon_F^{l_2-1}\right) - \sum_{r_3 \in R\left(2, \frac{1}{p}\mathcal{O}_F\right)} \chi_{K/F}(r_3 p\mathcal{O}_F) B_1(r_3) \right),$$

where ω_K is the number of roots of unity in K ([Shi76], Theorem 2).

We first simplify the coefficient term in this formula. Recall from Lemma 2.2 that $R_F/R_K = 1/2$. Since $K = \mathbb{Q}(\sqrt{d}, \sqrt{-p})$ for $p \geq 7$, we have $\omega_K = 2$. Furthermore, since we may choose the fundamental unit of F to be totally positive, we see that $\mathcal{O}_F^\times = \{\pm 1\} \times \mathcal{O}_F^{\times,+}$, so we get $[\mathcal{O}_F^\times : \mathcal{O}_F^{\times,+}] = 2$. Then,

$$\frac{2\omega_K R_F}{R_K \left[\mathcal{O}_F^\times : \mathcal{O}_F^{\times,+} \right]} = 1.$$

Next, we reindex the sum. First we split the set $R(1, \frac{1}{p}\mathcal{O}_F)$ into two parts. Consider the sets R_1, R_2 given by

$$\begin{aligned} R_1 &:= \left\{ (r_1, r_2) \in \mathbb{Q}^2 : 0 < r_1 \leq 1, 0 < r_2 < 1, r_1 + r_2\varepsilon_F \in \frac{1}{p}\mathcal{O}_F \right\} \\ R_2 &:= \left\{ (r_1, r_2) \in \mathbb{Q}^2 : 0 < r_1 \leq 1, r_2 = 1, r_1 + r_2\varepsilon_F \in \frac{1}{p}\mathcal{O}_F \right\}. \end{aligned}$$

Additionally, for simplicity we denote the inner sum of Shintani's formula by:

$$\mathcal{B}(r_1 + r_2\varepsilon_F) := \sum_{\substack{(l_1, l_2) \in \mathbb{Z}_{\geq 0}^2 \\ l_1 + l_2 = 2}} \frac{B_{l_1}(r_1)B_{l_2}(r_2)}{2 \cdot l_1!l_2!} \text{Tr}_{F/\mathbb{Q}}\left(\varepsilon_F^{l_2-1}\right).$$

By splitting the sum with $R(1, \frac{1}{p}\mathcal{O}_F) = R_1 \sqcup R_2$, we see that

$$\begin{aligned} h_K &= \sum_{r \in R_1} \chi_{K/F} \left((r_1 + r_2 \varepsilon_F) p \mathcal{O}_F \right) \mathcal{B}(r_1 + r_2 \varepsilon_F) \\ &\quad + \sum_{r \in R_2} \chi_{K/F} \left((r_1 + \varepsilon_F) p \mathcal{O}_F \right) \mathcal{B}(r_1 + \varepsilon_F) - \sum_{r \in R \left(2, \frac{1}{p} \mathcal{O}_F \right)} \chi_{K/F}(r p \mathcal{O}_F)(r - 1/2). \end{aligned} \quad (2.9)$$

Since $\varepsilon_F \in \mathcal{O}_F^\times$ and $\chi_{K/F}$ has conductor $p\mathcal{O}_F$, we have $\chi_{K/F}(r_1 p \mathcal{O}_F) = \chi_{K/F}((r_1 + \varepsilon_F) p \mathcal{O}_F)$. Moreover, comparing $\mathcal{B}(r_1)$ and $\mathcal{B}(r_1 + \varepsilon_F)$, we see that

$$\begin{aligned} \mathcal{B}(r_1) &= \frac{r_1^2 - r_1 + 1/3}{4} \text{Tr}_{F/\mathbb{Q}}(\varepsilon_F) - \frac{r_1 - 1/2}{2} \\ \mathcal{B}(r_1 + \varepsilon_F) &= \frac{r_1^2 - r_1 + 1/3}{4} \text{Tr}_{F/\mathbb{Q}}(\varepsilon_F) + \frac{r_1 - 1/2}{2} = \mathcal{B}(r_1) + r_1 - 1/2. \end{aligned}$$

Thus (2.9) simplifies to

$$h_K = \frac{1}{2} \sum_{r \in R_{F,p}} \chi_{K/F} \left((r_1 + r_2 \varepsilon_F) p \mathcal{O}_F \right) \sum_{\substack{(l_1, l_2) \in \mathbb{Z}_{\geq 0}^2 \\ l_1 + l_2 = 2}} \frac{B_{l_1}(r_1) B_{l_2}(r_2)}{l_1! l_2!} \text{Tr}_{F/\mathbb{Q}} \left(\varepsilon_F^{l_2 - 1} \right)$$

where $R_{F,p}$ is given by

$$R_{F,p} = \left\{ r = r_1 + r_2 \varepsilon_F : 0 < r_1 \leq 1, 0 \leq r_2 < 1, r \in \frac{1}{p} \mathcal{O}_F \right\}.$$

□

Definition 2.5. We call $R_{F,p}$ the *Shintani set* associated to F and p .

2.C. Properties of Shintani Sets

In this subsection, we identify a correspondence between $R_{F,p}$ and the finite field \mathbb{F}_{p^2} , which will play an important role in our proof of Theorem 1.1. Namely, we make use of this correspondence and the cyclic structure of the multiplicative group $\mathbb{F}_{p^2}^\times$ to enumerate the elements of $R_{F,p} - \mathcal{O}_F$ using the powers of a generator of $\mathbb{F}_{p^2}^\times$.

Throughout this subsection, we fix a totally real quadratic field F and an imaginary quadratic extension $K = F(\sqrt{-p})$, where $p \equiv 3 \pmod{4}$ and p remains inert in \mathcal{O}_F . We let $\varepsilon_F = s + t\theta_F$, and to simplify notation, we denote

$$\varepsilon := \varepsilon_F \quad \text{and} \quad R := R_{F,p}.$$

We begin by giving an explicit construction of the Shintani set:

Lemma 2.6. *The Shintani set R can be written as:*

$$R = \left\{ \frac{A}{tp} + \frac{B}{tp} \varepsilon : A + sB \equiv 0 \pmod{t}, A \in (0, tp] \cap \mathbb{Z}, B \in [0, tp) \cap \mathbb{Z} \right\}.$$

Proof. By Lemma 2.3, we have $D_{K/F} = p\mathcal{O}_F$. As such, for any element $r_1 + r_2\varepsilon \in \frac{1}{p}\mathcal{O}_F$, we have

$$r_1 + r_2\varepsilon = (r_1 + sr_2) + tr_2\theta_F \in \frac{1}{p}\mathcal{O}_F.$$

The set $\{1, \theta_F\}$ constitutes an integral basis of \mathcal{O}_F , meaning we can write any element of the Shintani set as $r_1 + r_2\varepsilon = \frac{A'}{p} + \frac{B}{p}\theta_F \in \frac{1}{p}\mathcal{O}_F$, for some $A', B \in \mathbb{Z}$. Note that

$$\frac{A'}{p} = r_1 + sr_2 \quad \text{and} \quad \frac{B}{p} = tr_2.$$

In particular, we have

$$r_2 = \frac{B}{tp},$$

and since $r_2 \in [0, 1)$, we see that $B \in [0, tp)$. Additionally, we see that

$$r_1 = \frac{A'}{p} - sr_2 = \frac{tA' - sB}{tp} = \frac{A}{tp}$$

where $A := tA' - sB$. We know that $r_1 \in (0, 1]$, so $A \in (0, tp]$. Moreover, since

$$\frac{A}{tp} + \frac{B}{tp}\varepsilon = \frac{A + sB}{tp} + \frac{B}{p}\theta_F \in \frac{1}{p}\mathcal{O}_F,$$

we must also have $A + sB \equiv 0 \pmod{t}$. From the expression above, we can see that every element of the form $\frac{A}{tp} + \frac{B}{tp}\varepsilon$ with $A, B \in \mathbb{Z}$, $A \in (0, tp]$, $B \in [0, tp)$, $A + sB \equiv 0 \pmod{t}$ is in the Shintani set. This finishes the proof. \square

Next, we want to identify R with the finite field \mathbb{F}_{p^2} . We begin with the work of Barquero-Sanchez, Masri, and Tsai, who proved that R is a finite abelian group with respect to the following operation:

$$r \oplus r' := r + r' + \mathbb{Z}[\varepsilon]$$

(see Proposition 4.3 in [BMT21]). This allows us to prove the following proposition relating R to \mathbb{F}_{p^2} , a property that is central to our proof of Theorem 1.1.

Proposition 2.7. *The Shintani set R has a structure as a $\mathbb{Z}[\varepsilon]$ -module. This structure admits a surjective $\mathbb{Z}[\varepsilon]$ -module homomorphism $\pi : R \rightarrow \mathbb{F}_{p^2}$.*

Proof. We begin with the $\mathbb{Z}[\varepsilon]$ -module structure on R . By definition, the fractional ideal $\frac{1}{p}\mathcal{O}_F$ is an \mathcal{O}_F -module, and since $\mathbb{Z}[\varepsilon]$ is a subring of \mathcal{O}_F , we observe that $\frac{1}{p}\mathcal{O}_F$ is a $\mathbb{Z}[\varepsilon]$ -module by restriction of scalars. Furthermore, since $\mathbb{Z}[\varepsilon]$ is a $\mathbb{Z}[\varepsilon]$ -submodule of $\frac{1}{p}\mathcal{O}_F$, we have that $\frac{1}{p}\mathcal{O}_F/\mathbb{Z}[\varepsilon]$ is a $\mathbb{Z}[\varepsilon]$ -module. Moreover, $R \subset \frac{1}{p}\mathcal{O}_F$ is a complete reduced set of coset representatives for $\frac{1}{p}\mathcal{O}_F/\mathbb{Z}[\varepsilon]$ (see Proposition 4.1 in [BMT21]). Thus R has the structure of a $\mathbb{Z}[\varepsilon]$ -module and can be identified with $\frac{1}{p}\mathcal{O}_F/\mathbb{Z}[\varepsilon]$.

Since $R \subseteq \frac{1}{p}\mathcal{O}_F$, multiplication by p defines an injective $\mathbb{Z}[\varepsilon]$ -module homomorphism

$$R \longrightarrow \mathcal{O}_F, \quad r \longmapsto pr + p\mathcal{O}_F.$$

If we compose this map with the projection $\mathcal{O}_F \longrightarrow \mathcal{O}_F/p\mathcal{O}_F$, we obtain the map

$$\pi : R \longrightarrow \mathcal{O}_F/p\mathcal{O}_F, \quad r \longmapsto pr,$$

which is surjective, as shown in Proposition 4.4 of [BMT21]. If p remains inert in F , then $p\mathcal{O}_F$ is prime and thus maximal, so $\mathcal{O}_F/p\mathcal{O}_F$ is a finite field. Then, since F is quadratic and $\mathcal{O}_F = \mathbb{Z}[\theta_F]$, we know that

$$\mathcal{O}_F/p\mathcal{O}_F \cong \mathbb{Z}[\theta_F]/p\mathbb{Z}[\theta_F] \cong \mathbb{F}_p[\theta] \cong \mathbb{F}_{p^2}.$$

\square

Remark. By the First Isomorphism Theorem,

$$R/\ker(\pi) \cong \mathcal{O}_F/p\mathcal{O}_F.$$

Note that this is an isomorphism of groups, and therefore pertains only to the structure of R as an additive abelian group. We do not require a multiplicative structure within R here; rather we point out that the map

$$\pi : R/\ker(\pi) \rightarrow \mathbb{F}_{p^2}$$

is bijective. We will make use of this bijective correspondence in the proof of Theorem 1.1.

Lemma 2.8. *The elements of $\ker(\pi)$ are exactly those elements of R which are in \mathcal{O}_F .*

Proof. Assume $r \in \ker(\pi)$. Then, since $\Im(\pi) = \mathcal{O}_F/p\mathcal{O}_F$, we have

$$\pi(r) = 0 \iff pr \in p\mathcal{O}_F \iff r \in \mathcal{O}_F.$$

□

Now we are in a position to explicitly describe the elements in $\ker(\pi)$.

Lemma 2.9. *The kernel of the map π is given by*

$$\ker(\pi) = \left\{ 1 - \left\{ \frac{si}{t} \right\}_{[0,1)} + \frac{i}{t}\varepsilon \mid 0 \leq i \leq t-1 \right\}$$

In particular, we have that $|\ker(\pi)| = t$.

Proof. Consider $r \in \ker(\pi)$. Using Lemma 2.6 and noting that $\varepsilon = s + t\theta_F$, we see that r has the form

$$r = \frac{A}{tp} + \frac{B}{tp}\varepsilon = \frac{A + sB}{tp} + \frac{B}{p}\theta_F.$$

By Lemma 2.8, $r \in \ker(\pi) \iff r \in R \cap \mathcal{O}_F$, so we have that $\frac{A+sB}{tp} \in \mathbb{Z}$ and $\frac{B}{p} \in \mathbb{Z}$. The second condition implies $p|B$, and since $B \in [0, tp) \cap \mathbb{Z}$ by Lemma 2.6, we see that $B = pi$ for $i \in [0, t) \cap \mathbb{Z}$. The condition that $\frac{A+sB}{tp} \in \mathbb{Z}$ implies that $A \equiv -sB = spi \pmod{tp}$. Since $A \in (0, tp) \cap \mathbb{Z}$ by Lemma 2.6, A is uniquely determined by B . More precisely,

$$A = tp - (spi \pmod{tp})$$

where $spi \pmod{tp}$ is the least positive residue of $spi \in \mathbb{Z}$ modulo tp . We can further simplify this expression; since

$$spi \pmod{tp} = spi - tp \left\lfloor \frac{spi}{tp} \right\rfloor,$$

we have that

$$\ker(\pi) \subseteq \left\{ 1 - \left\{ \frac{si}{t} \right\}_{[0,1)} + \frac{i}{t}\varepsilon : i \in [0, t) \cap \mathbb{Z} \right\},$$

where $\{\cdot\}$ denotes the fractional part function $\{x\}_I$, defined as the unique element of I satisfying $x - \{x\}_I \in \mathbb{Z}$. The converse containment is seen immediately from the fact that that $\varepsilon = s + t\theta_F$ and the definition of $spi \pmod{tp}$. Thus, $\ker(\pi)$ has size exactly t . □

We will denote the elements of $\ker(\pi)$ as

$$\kappa_i := 1 - \left\{ \frac{si}{t} \right\}_{[0,1)} + \frac{i}{t}\varepsilon \quad \text{for } i \in \{0, 1, \dots, t-1\}.$$

3. Proof of Theorem 1.1

Equipped with these facts about the Shintani set described in the previous section, we now prove Theorem 1.1. Our proof relies on features of the structure of the Shintani set which come from from the bijection between $R_{F,p}/\ker(\pi)$ and \mathbb{F}_{p^2} , as well as some properties we derive of the Hecke character across the Shintani set. Again, to simplify notation, we let $\varepsilon = \varepsilon_F$, $R = R_{F,p}$, and $\rho = \rho_{F,p}$.

We are now able to describe the Shintani set using the multiplicative structure of $\mathbb{F}_{p^2}^\times = \langle \rho + p\mathcal{O}_F \rangle$. Using the bijection from $R/\ker(\pi)$ to \mathbb{F}_{p^2} , we have

$$R = \ker(\pi) \sqcup \left(\bigsqcup_{m=1}^{p^2-1} \pi^{-1}(\rho^m + p\mathcal{O}_F) \right).$$

For each m between 1 and $p^2 - 1$, choose one element in the coset $\pi^{-1}(\rho^m + p\mathcal{O}_F)$, which we denote $\tilde{x}(m) + \tilde{y}(m)\varepsilon \in R$.

Next, we explicitly calculate each $\tilde{x}(m)$ and $\tilde{y}(m)$ in terms of ρ^m . Note that $\{1, \theta_F\}$ is a \mathbb{F}_p -basis of \mathbb{F}_{p^2} , so we can write $\rho^m + p\mathcal{O}_F := x(m) + y(m)\theta_F$ for some integers $x(m), y(m)$. Observe that, since $\varepsilon = s + t\theta_F$, we have

$$\rho^m + p\mathcal{O}_F = x(m) - \frac{s \cdot y(m)}{t} + \frac{y(m)}{t}\varepsilon.$$

Under multiplication by p and reduction modulo p , the point

$$\frac{x(m)}{p} - \frac{s \cdot y(m)}{tp} + \frac{y(m)}{tp}\varepsilon \in \frac{1}{p}\mathcal{O}_F$$

maps to $\rho^m + p\mathcal{O}_F$. Thus, if we subtract a suitable element of $\mathbb{Z}[\varepsilon]$ from this point, we obtain a point $\tilde{x}(m) + \tilde{y}(m)\varepsilon \in R$ that is a preimage of $\pi^{-1}(\rho^m + p\mathcal{O}_F)$. In particular, we see that

$$\tilde{x}(m) = \left\{ \frac{x(m)}{p} - \frac{s \cdot y(m)}{tp} \right\}_{(0,1]}, \quad \tilde{y}(m) = \left\{ \frac{y(m)}{tp} \right\}_{[0,1)}.$$

Since $\pi(\tilde{x}(m) + \tilde{y}(m)\varepsilon) = \rho^m + p\mathcal{O}_F$, we can construct the entire coset from this element:

$$\pi^{-1}(\rho^m + p\mathcal{O}_F) = \left\{ (\tilde{x}(m) + \tilde{y}(m)\varepsilon) \oplus \kappa_i : 1 \leq i \leq t \right\}.$$

For simplicity, we write

$$\tilde{x}_i(m) + \tilde{y}_i(m)\varepsilon := (\tilde{x}(m) + \tilde{y}(m)\varepsilon) \oplus \kappa_i. \tag{3.10}$$

Using our explicit construction of $\ker(\pi)$ given in Lemma 2.9, we can similarly explicitly construct each $\tilde{x}_i(m), \tilde{y}_i(m)$. We see that

$$\begin{aligned} \tilde{x}_i(m) &= \left\{ \frac{x(m)}{p} - \frac{s \cdot y(m)}{tp} + 1 - \left\{ \frac{si}{t} \right\}_{[0,1)} \right\}_{(0,1]} \\ \tilde{y}_i(m) &= \left\{ \frac{y(m)}{tp} + \frac{i}{t} \right\}_{[0,1)}. \end{aligned}$$

Thus, we can write R as the following disjoint union:

$$R = \ker(\pi) \sqcup \left(\bigsqcup_{m=1}^{p^2-1} \left\{ \tilde{x}_i(m) + \tilde{y}_i(m)\varepsilon : 1 \leq i \leq t \right\} \right).$$

By Proposition 2.4, we simplify Shintani's class number formula to obtain

$$h_K = \frac{1}{2} \sum_{\substack{1 \leq m \leq p^2-1 \\ 1 \leq i \leq t}} \chi_{K/F} \left((\tilde{x}_i(m) + \tilde{y}_i(m)\varepsilon) \cdot p\mathcal{O}_F \right) \cdot \sum_{\substack{0 \leq l_1, l_2 \leq 2 \\ l_1 + l_2 = 2}} \frac{B_{l_1}(\tilde{x}_i(m))}{l_1!} \frac{B_{l_2}(\tilde{y}_i(m))}{l_2!} \text{Tr}_{F/\mathbb{Q}}(\varepsilon_F)^{l_2-1}. \quad (3.11)$$

We can also simplify the Hecke character term. Consider any element $r_1 + r_2\varepsilon \in R$ and any element $k_1 + k_2\varepsilon \in \ker(\pi)$. By Lemma 2.8, we have $k_1 + k_2\varepsilon \in \mathcal{O}_F$. Since the Hecke character has conductor $p\mathcal{O}_F$, we have

$$\chi_{K/F} \left((r_1 + r_2\varepsilon + k_1 + k_2\varepsilon)p\mathcal{O}_F \right) = \chi_{K/F} \left(((r_1 + r_2\varepsilon)p\mathcal{O}_F) + p\mathcal{O}_F \right) = \chi_{K/F} \left((r_1 + r_2\varepsilon)p\mathcal{O}_F \right).$$

Thus, the value of $\chi_{K/F}(r_1 + r_2\varepsilon)$ depends only on the coset of $r_1 + r_2\varepsilon$ in $R/\ker(\pi)$. Therefore, we have that

$$\chi_{K/F} \left((\tilde{x}_i(m) + \tilde{y}_i(m)\varepsilon)p\mathcal{O}_F \right) = \chi_{K/F} \left((\tilde{x}(m) + \tilde{y}(m)\varepsilon)p\mathcal{O}_F \right).$$

By definition,

$$p(\tilde{x}(m) + \tilde{y}(m)\varepsilon) - \rho^m \in p\mathcal{O}_F.$$

Using this and the multiplicativity of the Hecke character, we get

$$\chi_{K/F}((\tilde{x}_i(m) + \tilde{y}_i(m)\varepsilon)p\mathcal{O}_F) = \chi_{K/F}((\rho^m + p\mathcal{O}_F)\mathcal{O}_F) = \chi_{K/F}((\rho + p\mathcal{O}_F)\mathcal{O}_F)^m.$$

If $\chi_{K/F}((\rho + p\mathcal{O}_F)\mathcal{O}_F) = 0$, then since $(\mathcal{O}_F/p\mathcal{O}_F)^\times = \langle \rho + p\mathcal{O}_F \rangle$, we would have that $\chi_{K/F}(rp\mathcal{O}_F) = 0$ for all $r \in R$. However, this contradicts the definition of $\chi_{K/F}$. Moreover, $\chi_{K/F}((\rho + p\mathcal{O}_F)\mathcal{O}_F) \neq 1$, since we would then similarly have that $\chi_{K/F}(rp\mathcal{O}_F) = 1$ for all $r \in R - \mathcal{O}_F$, but $\chi_{K/F}$ is a non-trivial character by construction. Thus, we see that $\chi_{K/F}((\rho + p\mathcal{O}_F)\mathcal{O}_F) = -1$, which implies

$$\chi_{K/F} \left((\tilde{x}_i(m) + \tilde{y}_i(m)\varepsilon)p\mathcal{O}_F \right) = \chi_{K/F}((\rho + p\mathcal{O}_F)\mathcal{O}_F)^m = (-1)^m.$$

Thus, Equation 3.11 simplifies further:

$$h_K = \frac{1}{2} \sum_{\substack{1 \leq m \leq p^2-1 \\ 1 \leq i \leq t}} (-1)^m \sum_{\substack{0 \leq l_1, l_2 \leq 2 \\ l_1 + l_2 = 2}} \frac{B_{l_1}(\tilde{x}_i(m))}{l_1!} \frac{B_{l_2}(\tilde{y}_i(m))}{l_2!} \text{Tr}_{F/\mathbb{Q}}(\varepsilon_F)^{l_2-1}.$$

Next, we simplify the Bernoulli polynomial part of the class number formula. We consider

$$\begin{aligned} & \sum_{\substack{0 \leq l_1, l_2 \leq 2 \\ l_1 + l_2 = 2}} \frac{B_{l_1}(\tilde{x}_i(m))}{l_1!} \frac{B_{l_2}(\tilde{y}_i(m))}{l_2!} \text{Tr}_{F/\mathbb{Q}}(\varepsilon)^{l_2-1} \\ &= \text{Tr}_{F/\mathbb{Q}}(\varepsilon) \frac{\tilde{x}_i(m)^2 - \tilde{x}_i(m) + 1/6}{2} + 2 \left(\tilde{x}_i(m) - \frac{1}{2} \right) \left(\tilde{y}_i(m) - \frac{1}{2} \right) + \text{Tr}_{F/\mathbb{Q}}(\varepsilon) \frac{\tilde{y}_i(m)^2 - \tilde{y}_i(m) + 1/6}{2} \\ &= \frac{\text{Tr}_{F/\mathbb{Q}}(\varepsilon)}{2} \left(\tilde{x}_i(m) - \frac{1}{2} \right)^2 + 4 \left(\tilde{x}_i(m) - \frac{1}{2} \right) \left(\tilde{y}_i(m) - \frac{1}{2} \right) + \frac{\text{Tr}_{F/\mathbb{Q}}(\varepsilon)}{2} \left(\tilde{y}_i(m) - \frac{1}{2} \right)^2 + c_0, \end{aligned}$$

for some constant c_0 . Since for any constant c ,

$$\sum_{\substack{1 \leq m \leq p^2-1 \\ 1 \leq i \leq t}} (-1)^m \cdot c = 0,$$

we can ignore the constant term c_0 that arises in the inner sum of Bernoulli polynomials. We can write the class number h_K as

$$h_K = \frac{1}{4} \sum_{\substack{1 \leq m \leq p^2-1 \\ 1 \leq i \leq t}} (-1)^m \left[\text{Tr}_{F/\mathbb{Q}}(\varepsilon) \left(\tilde{x}_i(m) - \frac{1}{2} \right)^2 + 4 \left(\tilde{x}_i(m) - \frac{1}{2} \right) \left(\tilde{y}_i(m) - \frac{1}{2} \right) + \text{Tr}_{F/\mathbb{Q}}(\varepsilon) \left(\tilde{y}_i(m) - \frac{1}{2} \right)^2 \right]. \quad (3.12)$$

If we define

$$x_i(m) := tp(2\tilde{x}_i(m) - 1) \quad \text{and} \quad y_i(m) := tp(2\tilde{y}_i(m) - 1), \quad (3.13)$$

we can then rewrite the above equation as

$$h_K = \frac{1}{16t^2p^2} \sum_{\substack{1 \leq m \leq p^2-1 \\ 1 \leq i \leq t}} (-1)^m \left[\text{Tr}_{F/\mathbb{Q}}(\varepsilon) \left(x_i(m) \right)^2 + 4 \left(x_i(m) \right) \left(y_i(m) \right) + \text{Tr}_{F/\mathbb{Q}}(\varepsilon) \left(y_i(m) \right)^2 \right]. \quad (3.14)$$

Finally, by defining the quadratic form

$$Q_F(Y_1, Y_2) := \text{Tr}_{F/\mathbb{Q}}(\varepsilon)Y_1^2 + 4Y_1Y_2 + \text{Tr}_{F/\mathbb{Q}}(\varepsilon)Y_2^2,$$

we rewrite (3.14) as

$$h_K = \frac{1}{16t^2p^2} \sum_{\substack{1 \leq m \leq p^2-1 \\ 1 \leq i \leq t}} (-1)^m Q_F(x_i(m), y_i(m)). \quad (3.15)$$

The last step is to derive recurrence relations for $x(m), y(m)$, the coefficients of $\rho^m + p\mathcal{O}_F = x(m) + y(m)\theta_F$. The minimal polynomial of θ_F is $x^2 - \text{Tr}(\theta_F)x + \text{Norm}_{F/\mathbb{Q}}(\theta_F)$, which implies

$$\theta_F^2 = \text{Tr}_{F/\mathbb{Q}}(\theta_F)\theta_F - \text{Norm}_{F/\mathbb{Q}}(\theta_F).$$

To simplify notation, let $T = \text{Tr}_{F/\mathbb{Q}}(\theta_F)$ and $N = \text{Norm}_{F/\mathbb{Q}}(\theta_F)$. Since $\rho := a + b\varepsilon$, we have the initial conditions $x(1) = a$ and $y(1) = b$. Then, we get

$$\begin{aligned} \rho^{m+1} &= x(m+1) + y(m+1)\theta_F = (x(m) + y(m)\theta_F) \cdot (a + b\theta_F) \\ &= a \cdot x(m) - Nb \cdot y(m) + \left(b \cdot x(m) + (a + Tb) \cdot y(m) \right) \theta_F. \end{aligned}$$

This implies the following recurrence relations:

$$\begin{aligned} x(m+1) &= a \cdot x(m) - Nb \cdot y(m) \\ y(m+1) &= b \cdot x(m) + (a + Tb) \cdot y(m). \end{aligned}$$

Then, consider functions $X(z), Y(z)$ given by

$$X(z) = \sum_{m=1}^{\infty} x(m) \cdot z^m, \quad Y(z) = \sum_{m=1}^{\infty} y(m) \cdot z^m. \quad (3.16)$$

Using our recurrence relations, we can set up a system of equations to find explicit expressions for $X(z), Y(z)$ as rational functions determined by $x(1)$ and $y(1)$. We see that

$$\begin{aligned} X(z) &= z \cdot [a \cdot X(z) - Nb \cdot Y(z)] + az \\ Y(z) &= z \cdot \left[b \cdot X(z) + (a + Tb) \cdot Y(z) \right] + bz, \end{aligned}$$

which gives

$$X(z) = \frac{az - (a^2 + abT + Nb^2)z^2}{(a^2 + abT + Nb^2)z^2 - (2a + bT)z + 1}$$

$$Y(z) = \frac{bz}{(a^2 + abT + b^2N)z^2 - (2a + bT)z + 1}.$$

We simplify these by letting $C_{F,p} := a^2 + abT + Nb^2$ and $D_{F,p} := 2a + bT$ to get

$$X(z) = \frac{az - C_{F,p}z^2}{C_{F,p}z^2 - D_{F,p}z + 1}, \quad Y(z) = \frac{bz}{C_{F,p}z^2 - D_{F,p}z + 1}.$$

Note that the coefficients $x(m), y(m)$ of the power series of these rational functions correspond to those $x_i(m), y_i(m)$ which we use to generate each $x_i(m), y_i(m)$ using the formulas

$$x_i(m) := tp(2\tilde{x}_i(m) - 1) \quad \text{and} \quad y_i(m) := tp(2\tilde{y}_i(m) - 1).$$

This concludes the proof of Theorem 1.1.

4. Proof of Theorem 1.2

Here we prove Theorem 1.2, which relies heavily on the structure of the Shintani set as a $\mathbb{Z}[\varepsilon_F]$ -module and the related attributes of the base- ε_F expansions of its elements. Through a series of preliminary lemmas, we set up the proof of Theorem 1.2 by relating the base- ε_F expansion of $1/p$ to the orbit of elements in $R_{F,p} - \ker(\pi)$ under the action of ε_F . This allows us to derive a finite sum analogous to Girstmair's (1.2), in which the number of summands is equal to the period length of the base ε_F expansion of $1/p$.

Throughout this section, we fix a totally real quadratic field F and an imaginary quadratic extension $K := F(\sqrt{-p})$, where $p \equiv 3 \pmod{4}$ and p remains inert in \mathcal{O}_F . To simplify notation, we also let

$$\varepsilon := \varepsilon_F \quad \text{and} \quad R := R_{F,p}.$$

Additionally, we denote $r \in R$ as $r := r_1 + r_2\varepsilon$.

4.A. Shintani Cycles

Recall from Section 2 that we can identify R with $\frac{1}{p}\mathcal{O}_F/\mathbb{Z}[\varepsilon]$ to make it into a $\mathbb{Z}[\varepsilon]$ module. In particular, the multiplicative group $\langle \varepsilon \rangle$ acts on $\frac{1}{p}\mathcal{O}_F$ via scalar multiplication. If we denote the map for this group action by

$$\mu : \langle \varepsilon \rangle \times \frac{1}{p}\mathcal{O}_F \longrightarrow \frac{1}{p}\mathcal{O}_F,$$

we can compose μ with the projection map

$$\nu : \frac{1}{p}\mathcal{O}_F \longrightarrow \frac{1}{p}\mathcal{O}_F/\mathbb{Z}[\varepsilon]$$

to yield

$$\mu' := \nu \circ \mu : \langle \varepsilon \rangle \times \frac{1}{p}\mathcal{O}_F \longrightarrow \frac{1}{p}\mathcal{O}_F/\mathbb{Z}[\varepsilon].$$

Note that, since ν is a $\mathbb{Z}[\varepsilon]$ -module homomorphism, μ' constitutes a group action of $\langle \varepsilon \rangle$ on $\frac{1}{p}\mathcal{O}_F/\mathbb{Z}[\varepsilon]$.

Lemma 4.1. *The map*

$$\bar{\mu} : \langle \varepsilon \rangle \times \frac{1}{p} \mathcal{O}_F / \mathbb{Z}[\varepsilon] \longrightarrow \frac{1}{p} \mathcal{O}_F / \mathbb{Z}[\varepsilon], \quad (\varepsilon, \alpha + \mathbb{Z}[\varepsilon]) \longmapsto \mu'(\varepsilon, \alpha)$$

is a well-defined group action.

Proof. Since μ' is a group action, it is sufficient to show that $\bar{\mu}$ is well-defined. Take $\alpha, \alpha' \in \frac{1}{p} \mathcal{O}_F$ such that $\alpha + \mathbb{Z}[\varepsilon] = \alpha' + \mathbb{Z}[\varepsilon]$. Thus, for any $n \in \mathbb{Z}$, we have

$$\begin{aligned} \bar{\mu}(\varepsilon^n, \alpha + \mathbb{Z}[\varepsilon]) &= \mu'(\varepsilon^n, \alpha + \mathbb{Z}[\varepsilon]) \\ &= \varepsilon^n \alpha + \mathbb{Z}[\varepsilon] = \varepsilon^n \alpha' + \mathbb{Z}[\varepsilon] \\ &= \bar{\mu}(\varepsilon^n, \alpha' + \mathbb{Z}[\varepsilon]). \end{aligned}$$

Thus, $\bar{\mu}$ is well-defined, so $\bar{\mu}$ constitutes a group action of $\langle \varepsilon \rangle$ on $\frac{1}{p} \mathcal{O}_F / \mathbb{Z}[\varepsilon]$. \square

We know from Proposition 4.1 in [BMT21] that R is a complete and reduced set of representatives of $\frac{1}{p} \mathcal{O}_F / \mathbb{Z}[\varepsilon]$. Thus, we obtain a group action $\langle \varepsilon \rangle \curvearrowright R$ given by $(\varepsilon, r) \mapsto \varepsilon * r$, where $\varepsilon * r = \varepsilon r + z$, and z is the unique element of $\mathbb{Z}[\varepsilon]$ such that $\varepsilon r + z \in R$. We define the *Shintani cycle* of any element $r \in R$ to be the orbit of r under this action, and we denote this set as $C_r := \langle \varepsilon \rangle * r$.

Remark. Note that $\varepsilon * r \in \mathcal{O}_F \iff r \in \mathcal{O}_F$. Thus, for any $r \in R \cap \mathcal{O}_F$, every element in the Shintani cycle of r is an element of \mathcal{O}_F . We will call Shintani cycles containing elements in $R - \mathcal{O}_F$ the *nontrivial Shintani cycles* of R . We refer to Shintani cycles of elements in $R \cap \mathcal{O}_F$ as *trivial Shintani cycles* because the elements in these cycles are weighted by a factor of 0 in Shintani's class number formula (see the remark in Section 4.C), and hence for our purposes are “trivial.”

4.B. Epsilon Expansions

A base- ε expansion is an analogue to the usual decimal expansion. The base- ε expansion of any element $\alpha \in F$ is computed in the following way. Let $n := \lfloor \log_\varepsilon(\alpha) \rfloor$. Then we have

$$\alpha = a_n \varepsilon^n + a_{n-1} \varepsilon^{n-1} + \cdots + a_0 + a_{-1} \varepsilon^{-1} + \cdots,$$

where

$$a_n := \lfloor \alpha / \varepsilon^n \rfloor, a_{n-1} := \lfloor (\alpha - a_n \varepsilon^n) / \varepsilon^{n-1} \rfloor, \dots, a_i := \lfloor (\alpha - a_n \varepsilon^n - \cdots - a_{i+1} \varepsilon^{i+1}) / \varepsilon^i \rfloor, \dots$$

We observe that ε is an algebraic integer which is real since F is real quadratic, and that ε must be > 1 since it is a totally positive fundamental unit. Moreover, ε must have Galois conjugate with absolute value < 1 since F is a real quadratic field and ε has norm 1. Thus, ε is a Pisot number by definition, and by consequence, Theorem 3.1 in [Sch80] shows that any element of R has an eventually periodic base- ε expansion.

For some $\alpha \in F$ whose base ε expansion can be written as

$$\alpha = a_n \varepsilon^n + \cdots + a_0 + a_{-1} \varepsilon^{-1} + \cdots + a_{-k} \varepsilon^{-k} + \overline{a_{-k-1} \varepsilon^{-k-1} + \cdots + a_{-k-P_\alpha} \varepsilon^{-k-P_\alpha}},$$

we call P_α the *period length* of the base- ε expansion of α . Additionally, we will call the ordered set

$$\{a_{-k-1}, \dots, a_{-k-P_\alpha}\}$$

the *period set* of the base- ε expansion of α . We can further observe that any element of F whose base- ε expansion is finite is an element of $\mathbb{Z}[\varepsilon]$, by the following argument.

Lemma 4.2. *If $\alpha \in F$ has a finite base- ε expansion, then $\alpha \in \mathbb{Z}[\varepsilon]$.*

Proof. If γ has a finite base- ε expansion, we can express it as

$$\gamma = \sum_{i=K_1}^{K_2} m_i \varepsilon^i$$

where K_1, K_2 are integers. Using that $\varepsilon^2 = \text{Tr}_{F/\mathbb{Q}}(\varepsilon)\varepsilon - 1$ and that $\varepsilon^{-1} = \text{Tr}_{F/\mathbb{Q}}(\varepsilon) - \varepsilon$, we can perform the following replacement on any term $m_k \varepsilon^k$ where $k \neq 0$ or 1 :

$$m_k \varepsilon^k = \begin{cases} m_k (\text{Tr}_{F/\mathbb{Q}}(\varepsilon)\varepsilon - 1)^{k/2} & \text{if } k \text{ is an even positive integer} \\ m_k (\text{Tr}_{F/\mathbb{Q}}(\varepsilon)\varepsilon - 1)^{(k-1)/2} \varepsilon & \text{if } k \text{ is an odd positive integer} \\ m_k (\text{Tr}_{F/\mathbb{Q}}(\varepsilon) - \varepsilon)^{-k} & \text{if } k \text{ is a negative integer.} \end{cases}$$

The third equality implies that any negative integer power of ε can be converted to a linear combination of positive integer powers of ε . Therefore, it suffices to show that a linear combination of positive integer powers of ε can be expressed as an element of $\mathbb{Z}[\varepsilon]$. The first two equalities guarantee that any positive power of ε can be expressed a strictly lower positive power of ε . Thus by induction, any finite linear combination of (possibly negative) powers of ε can be expressed as an element of $\mathbb{Z}[\varepsilon]$. \square

Proposition 4.3. *The repeating part in the base- ε expansion of any two elements in the same Shintani cycle is the same.*

To prove this lemma, we require some preliminaries. Consider some $r \in R$, where $r = r_1 + r_2\varepsilon$, and recall that $0 < r_1 \leq 1$ and $0 \leq r_2 < 1$, $r_1, r_2 \in \mathbb{Q}$. Hence the action of ε on R amounts to:

$$\varepsilon * r = \varepsilon \cdot (r_1 + r_2\varepsilon) + z_1 + z_2\varepsilon$$

where $z_1 + z_2\varepsilon$ is the unique element in $\mathbb{Z}[\varepsilon]$ such that $\varepsilon \cdot (r_1 + r_2\varepsilon) + z_1 + z_2\varepsilon \in R$. We can explicitly compute bounds for z_1 and z_2 :

Lemma 4.4. *If $\varepsilon * (r_1 + r_2\varepsilon) = \varepsilon \cdot (r_1 + r_2\varepsilon) + z_1 + z_2\varepsilon$, then*

$$z_1 = 1, \quad \text{and} \quad z_2 = -\lfloor r_1 + r_2 \text{Tr}_{F/\mathbb{Q}}(\varepsilon) \rfloor.$$

Proof. The minimal polynomial of ε is

$$x^2 - \text{Tr}_{F/\mathbb{Q}}(\varepsilon)x + \text{Norm}_{F/\mathbb{Q}}(\varepsilon) = x^2 - \text{Tr}_{F/\mathbb{Q}}(\varepsilon)x + 1,$$

and thus

$$\varepsilon^2 = \text{Tr}_{F/\mathbb{Q}}(\varepsilon)\varepsilon - 1.$$

Consider

$$\varepsilon(r_1 + r_2\varepsilon) = r_1\varepsilon + r_2\varepsilon^2 = -r_2 + (r_1 + r_2 \text{Tr}_{F/\mathbb{Q}}(\varepsilon))\varepsilon.$$

To find $\varepsilon * (r_1 + r_2\varepsilon)$, we must shift $\varepsilon(r_1 + r_2\varepsilon)$ by some $z_1 + z_2\varepsilon \in \mathbb{Z}[\varepsilon]$ such that

$$-r_2 + z_1 \in (0, 1], \quad \text{and} \quad r_1 + r_2 \text{Tr}_{F/\mathbb{Q}}(\varepsilon) + z_2 \in [0, 1).$$

It is immediately apparent that $z_2 = -\lfloor r_1 + r_2 \text{Tr}_{F/\mathbb{Q}}(\varepsilon) \rfloor$. Further, since $r_1 + r_2\varepsilon \in R$, we have that $r_2 \in [0, 1)$, so we see that $z_1 = 1$. \square

Note that the above proposition and our bounds on r_1 and r_2 imply that $-\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) \leq z_2 \leq 0$. Before we show that the repeating part of the base ε of elements in the same Shintani cycle is the same, we require one more fact about ε , which we now prove.

Lemma 4.5. *We have that $[\varepsilon] = \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon)$.*

Proof. Let $\varepsilon = s + t\sqrt{d}$. We start by showing $\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) \geq [\varepsilon]$. Observe that

$$\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) = \varepsilon + \frac{1}{\varepsilon} \implies \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) > \varepsilon \implies \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) \geq [\varepsilon],$$

because the trace of an algebraic integer is always an element of \mathbb{Z} .

Now we will show that $\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) \leq [\varepsilon]$. Assume for the sake of contradiction that $\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) \geq [\varepsilon] + 1$. Then we have that

$$\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) \geq [\varepsilon] + 1 \implies \frac{\varepsilon^2 + 1}{\varepsilon} \geq [\varepsilon] + 1 \implies 1 - \varepsilon \geq \varepsilon[\varepsilon] - \varepsilon^2 \geq 0 \implies 1 \geq \varepsilon.$$

However, by definition, $\varepsilon > 1$, so we see that

$$\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) < [\varepsilon] + 1 \implies \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) \leq [\varepsilon].$$

□

Now we proceed to prove that the repeating part in the base- ε expansion of any two elements in the same Shintani cycle is the same.

Proof of Proposition 4.3. Consider some element $r \in R$, with base- ε expansion

$$r = a_1\varepsilon + a_0 + a_{-1}\varepsilon^{-1} + a_{-2}\varepsilon^{-2} + a_{-3}\varepsilon^{-3} + \dots$$

Note that since $r \in R$, $[\log_\varepsilon(r)] = 0$ or 1 , so the highest power of ε appearing in the base- ε expansion of r is at most 1 . Given this base- ε expansion of r , we have that

$$\varepsilon * r = \varepsilon \cdot r + z_2\varepsilon + 1 = a_1\varepsilon^2 + (a_0 + z_2)\varepsilon^1 + (a_{-1} + 1)\varepsilon^0 + a_{-2}\varepsilon^{-1} + a_{-3}\varepsilon^{-2} + \dots \quad (4.17)$$

Recall that in a base- ε expansion, each digit (in this case a_i for $i \in \mathbb{Z}$) must be an element of the set $A := \{0, 1, \dots, [\varepsilon]\}$. We now consider the following two cases: in Case 1, both $a_0 + z_2$ and $a_{-1} + 1$ are in A ; in Case 2, one or both of $a_0 + z_2$ and $a_{-1} + 1$ is not in A .

Case 1. In Case 1, the expression in (4.17) is already a valid base- ε expansion of $\varepsilon * r$. We can see that only a finite number of digits differ between the base- ε expansion of $\varepsilon * r$ and the base- ε expansion of r , so in this case the repeating part of $\varepsilon * r$ must be the same as r .

Case 2. Now we address Case 2, which we can split into Case 2.1 and Case 2.2. In Case 2.1, $a_0 + z_2 \notin A$; in Case 2.2, $a_{-1} + 1 \notin A$.

Case 2.1. Assume that $a_0 + z_2 \notin A$. Since a_0 is a digit in the base- ε expansion of r , $0 \leq a_0 \leq [\varepsilon]$ by definition. Additionally, $-\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) \leq z_2 \leq 0$ by Lemma 4.4. Thus it is always true that $-\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) \leq a_0 + z_2 \leq \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon)$. Therefore if $a_0 + z_2 \notin A$, it must be that $-\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) \leq a_0 + z_2 \leq -1$. Then we have that $0 \leq a_0 + z_2 + \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) \leq \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) - 1$, so $a_0 + z_2 + \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) \in A$ and is hence an acceptable digit. Since $\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon) = \varepsilon + \varepsilon^{-1}$, we can rewrite (4.17) as

$$\begin{aligned} \varepsilon * r &= (a_1 - 1)\varepsilon^2 + (a_0 + z_2 + \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon))\varepsilon + (a_{-1} + 1 - 1) + a_{-2}\varepsilon^{-1} + a_{-3}\varepsilon^{-2} + \dots \\ &= (a_1 - 1)\varepsilon^2 + (a_0 + z_2 + \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon))\varepsilon + a_{-1} + a_{-2}\varepsilon^{-1} + a_{-3}\varepsilon^{-2} + \dots \end{aligned} \quad (4.18)$$

Since $0 \leq a_0 + z_2 + \text{Tr}_{F/\mathbb{Q}}(\varepsilon) < \text{Tr}_{F/\mathbb{Q}}(\varepsilon)$, the above base- ε expansion is valid as long as $0 \leq a_1 - 1 \leq \lfloor \varepsilon \rfloor$. Since $0 \leq a_1 \leq \lfloor \varepsilon \rfloor$, we know $-1 \leq a_1 - 1 \leq \lfloor \varepsilon \rfloor - 1$. Thus unless $a_1 - 1 = -1$, it must be true that $0 \leq a_1 - 1 \leq \lfloor \varepsilon \rfloor$. Let us assume for the sake of contradiction that $a_1 - 1 = -1$. If we let

$$\begin{aligned} \alpha &= \varepsilon^2 \text{ and} \\ \beta &= (a_0 + z_2 + \text{Tr}_{F/\mathbb{Q}}(\varepsilon))\varepsilon + a_{-1} + a_{-2}\varepsilon^{-1} + a_{-3}\varepsilon^{-2} + \dots, \end{aligned}$$

then (4.18) implies that $\varepsilon * r = -\alpha + \beta$. However, it follows directly from the definition of a base- ε expansion and the fact that ε is a Pisot number that $\alpha > \beta$. Thus $\varepsilon * r = -\alpha + \beta < 0$, which contradicts the fact that $\varepsilon * r \in R$. Thus we have that $0 \leq a_1 - 1 \leq \lfloor \varepsilon \rfloor$, so (4.18) is a valid base- ε expansion of $\varepsilon * r$. We can see that only a finite number of digits differ between the base- ε expansion of $\varepsilon * r$ and the base- ε expansion of r . Therefore the repeating part of $\varepsilon * r$ must be the same as r .

Case 2.2 Assume $a_{-1} + 1 \notin A$. By Case 2.1, we may assume without loss of generality that $a_0 + z_2 \in A$. Since $0 \leq a_{-1} \leq \lfloor \varepsilon \rfloor$, we know that $1 \leq a_{-1} + 1 \leq \lfloor \varepsilon \rfloor + 1$. Thus if $a_{-1} + 1 \notin A$, it must be that $a_{-1} + 1 = \lfloor \varepsilon \rfloor + 1$, so $a_{-1} = \lfloor \varepsilon \rfloor$. Since $\lfloor \varepsilon \rfloor = \text{Tr}_{F/\mathbb{Q}}(\varepsilon)$ by Lemma 4.5, we have $a_{-1} + 1 = \text{Tr}_{F/\mathbb{Q}}(\varepsilon)$. Again using that $\text{Tr}_{F/\mathbb{Q}}(\varepsilon) = \varepsilon + \varepsilon^{-1}$, we can rewrite (4.17) as

$$\varepsilon * r = a_1\varepsilon^2 + (a_0 + z_2 + 1)\varepsilon + (a_{-2} + 1)\varepsilon^{-1} + a_{-3}\varepsilon^{-2} + \dots \quad (4.19)$$

Since $0 \leq a_0 + z_2 \leq \lfloor \varepsilon \rfloor$ by assumption, if $a_0 + z_2 + 1 \notin A$, then $a_0 + z_2 + 1 = \lfloor \varepsilon \rfloor + 1$. This would imply that $\varepsilon * r > \varepsilon + 1$, which contradicts the fact that $\varepsilon * r \in R$. Thus it must be that $0 \leq a_0 + z_2 + 1 \leq \lfloor \varepsilon \rfloor$. With this, we see that if $a_{-2} + 1 \in A$, then 4.19 is a valid base- ε expansion of $\varepsilon * r$. Otherwise, if $a_{-2} + 1 \notin A$, then since $a_{-2} \in A$, it must be that $a_{-2} = \lfloor \varepsilon \rfloor$, so $a_{-2} + 1 = \lfloor \varepsilon \rfloor + 1 = \text{Tr}_{F/\mathbb{Q}}(\varepsilon)$. Using that $\text{Tr}_{F/\mathbb{Q}}(\varepsilon) = \varepsilon + \varepsilon^{-1}$, we can rewrite 4.19 as

$$\varepsilon * r = a_1\varepsilon^2 + (a_0 + z_2 + 1)\varepsilon + 1 + (a_{-3} + 1)\varepsilon^{-2} + \dots \quad (4.20)$$

We note that by the same argument used before, if $a_i + 1 \notin A$ for any $i \in \mathbb{Z}$, then $a_i = \lfloor \varepsilon \rfloor = \text{Tr}_{F/\mathbb{Q}}(\varepsilon) - 1$. Thus if we let j be the smallest positive integer such that $a_{-j} \neq \lfloor \varepsilon \rfloor$, then continuing in the same manner, we see that

$$\varepsilon * r = a_1\varepsilon^2 + (a_0 + z_2 + 1)\varepsilon + 1 + \varepsilon^{-1} + \varepsilon^{-2} + \dots + \varepsilon^{-j+3} + (a_j + 1)\varepsilon^{-j+1} + a_{j+1}\varepsilon^{-j} \dots \quad (4.21)$$

Since the base- ε expansion of r must be finite or periodic, it is certainly possible to choose such an index j . We can assume that r does not have repeating part $\overline{\lfloor \varepsilon \rfloor}$, since $\lfloor \varepsilon \rfloor \varepsilon^i + \lfloor \varepsilon \rfloor \varepsilon^{i-1} + \lfloor \varepsilon \rfloor \varepsilon^{i-2} + \dots = \varepsilon^{i+1}$ for any $i \in \mathbb{Z}$. Thus in Case 2.2, we see that only a finite number of digits differ between the base- ε expansion of $\varepsilon * r$ and the base- ε expansion of r . Therefore the repeating part of $\varepsilon * r$ must be the same as r in this case.

Now we have seen that in all cases, the repeating part of the base- ε expansion of $\varepsilon * r$ is the same as that of r , which finishes the proof. \square

In many of the results which follow, it will prove useful for us to note the following fact about the map π as defined in Proposition 2.7.

Lemma 4.6. *The map π is equivariant under the action of $\langle \varepsilon \rangle$.*

Proof. Since $\frac{1}{p}\mathcal{O}_F$ is an ideal of \mathcal{O}_F , it is also a \mathcal{O}_F -module. Moreover, \mathcal{O}_F is trivially an \mathcal{O}_F -module, and $p\mathcal{O}_F$ is a submodule of \mathcal{O}_F since $p\mathcal{O}_F$ is an ideal of \mathcal{O}_F . Thus the map

$$\phi : \frac{1}{p}\mathcal{O}_F \rightarrow \mathcal{O}_F/p\mathcal{O}_F$$

defined by multiplication by p is an \mathcal{O}_F -module homomorphism. The kernel of this map is \mathcal{O}_F , so by the first isomorphism theorem, $\frac{1}{p}\mathcal{O}_F/\mathcal{O}_F \xrightarrow{\sim} \mathcal{O}_F/p\mathcal{O}_F$ is an isomorphism of \mathcal{O}_F -modules. Since

$\mathbb{Z}[\varepsilon]$ is a subring of \mathcal{O}_F , by restriction of scalars, $\frac{1}{p}\mathcal{O}_F/\mathcal{O}_F \cong \mathcal{O}_F/p\mathcal{O}_F$ is also an isomorphism of $\mathbb{Z}[\varepsilon]$ -modules.

We can also observe that since \mathcal{O}_F is a submodule of $\frac{1}{p}\mathcal{O}_F$, the projection map

$$\frac{1}{p}\mathcal{O}_F/\mathbb{Z}[\varepsilon] \rightarrow \frac{1}{p}\mathcal{O}_F/\mathbb{Z}[\varepsilon] \Big/ \mathcal{O}_F/\mathbb{Z}[\varepsilon]$$

is a surjective $\mathbb{Z}[\varepsilon]$ -module homomorphism. By the third isomorphism theorem, we further have that

$$\frac{1}{p}\mathcal{O}_F/\mathbb{Z}[\varepsilon] \Big/ \mathcal{O}_F/\mathbb{Z}[\varepsilon] \cong \frac{1}{p}\mathcal{O}_F/\mathcal{O}_F,$$

which implies

$$\psi : \frac{1}{p}\mathcal{O}_F/\mathbb{Z}[\varepsilon] \rightarrow \frac{1}{p}\mathcal{O}_F/\mathcal{O}_F$$

is a surjective $\mathbb{Z}[\varepsilon]$ -module homomorphism. Since $R \subset \frac{1}{p}\mathcal{O}_F$ and R constitutes a complete set of coset representatives for $\frac{1}{p}\mathcal{O}_F/\mathbb{Z}[\varepsilon]$ (see [BMT21], Proposition 4.1), the identity map

$$\iota : R \rightarrow \frac{1}{p}\mathcal{O}_F/\mathbb{Z}[\varepsilon]$$

is a $\mathbb{Z}[\varepsilon]$ -module isomorphism. Now we can see that since $\pi = \phi \circ \psi \circ \iota$, π is a surjective $\mathbb{Z}[\varepsilon]$ -module homomorphism. Thus π is equivariant under the action of $\langle \varepsilon \rangle$. \square

With this result, we may now examine more closely the action of ε on R . Namely, we can deduce the following fact about nontrivial Shintani cycles.

Lemma 4.7. *All nontrivial Shintani cycles have length equal to the multiplicative order of $\varepsilon + p\mathcal{O}_F$ in $(\mathcal{O}_F/p\mathcal{O}_F)$.*

Proof. Let M denote the multiplicative order of $\varepsilon + p\mathcal{O}_F$ in $\mathcal{O}_F/p\mathcal{O}_F$, and consider $r \in R - \mathcal{O}_F$. We will show that $|C_r| = M$. Suppose that $\varepsilon^m * r = r$ for some $m \in \mathbb{Z}^+$. Then by Lemma 4.6,

$$\pi(r) = \pi(\varepsilon^m * r) = (\varepsilon^m + p\mathcal{O}_F)\pi(r) \implies (\varepsilon^m - 1 + p\mathcal{O}_F)\pi(r) = 0.$$

By assumption $r \notin \mathcal{O}_F$, so $\pi(r) \neq 0$ by Lemma 2.8. Since $\mathcal{O}_F/p\mathcal{O}_F$ is a field, it must be that $(\varepsilon^m - 1 + p\mathcal{O}_F) = 0$. Therefore $\varepsilon^m \equiv 1 \pmod{p\mathcal{O}_F}$, so $M|m$. As a consequence, if we denote the stabilizer subgroup associated to r under the action of ε as $\langle \varepsilon \rangle_r$, then $\langle \varepsilon \rangle_r \subset \langle \varepsilon^M \rangle$. Moreover, we note that since $\langle \varepsilon \rangle_r$ is a subgroup of $\langle \varepsilon^M \rangle$, it must be that $\langle \varepsilon \rangle_r = \langle \varepsilon^{M'} \rangle$ for some M' such that $M|M'$. Moreover, we also have that

$$\varepsilon^{M'} * r = r \implies (\varepsilon^{M'} - 1 + p\mathcal{O}_F)\pi(r) = 0$$

where $\pi(r) \neq 0$, so that $\varepsilon^{M'} \equiv 1 \pmod{p\mathcal{O}_F}$. Thus it must also be that $M'|M$, so $M' = M$, and hence $\langle \varepsilon \rangle_r = \langle \varepsilon^M \rangle$. In other words, $\langle \varepsilon^M \rangle$ is the stabilizer subgroup of r for all $r \in R - \mathcal{O}_F$. By the orbit-stabilizer theorem, we then have that $|C_r| = [\langle \varepsilon \rangle : \langle \varepsilon^M \rangle] = M$. \square

In the lemma which follows, we equate M with the minimal period length of the base- ε expansion of r for all $r \in R - \mathcal{O}_F$. This fact, combined with Lemma 4.7, will then imply that for all $r \in R - \mathcal{O}_F$, $|C_r| = P_r$, where P_r denotes the minimal period length of the base- ε expansion of r .

Lemma 4.8. *For any $r \in R - \mathcal{O}_F$, the minimal period length of the base- ε expansion of r is equal to the multiplicative order of $\varepsilon + p\mathcal{O}_F$ in $(\mathcal{O}_F/p\mathcal{O}_F)$.*

Proof. Consider an element $r = r_1 + r_2\varepsilon \in R - \mathcal{O}_F$. We start by showing that $P_r | M$. As mentioned at the beginning of Section 4.B, the base- ε expansion of r is always eventually periodic, say

$$r = \sum_{i=-1}^{N-1} a'_i \varepsilon^{-i} + \varepsilon^{-N} \sum_{j=0}^{\infty} (a_1 \varepsilon^{-jP_r} + a_2 \varepsilon^{-jP_r-1} + \dots + a_{P_r} \varepsilon^{-jP_r-P_r+1}). \quad (4.22)$$

We remind the reader that since $r \in R$, $[\log_\varepsilon(r)] = 0$ or 1 , so the highest power of ε in (4.22) is 1 . Multiplying (4.22) by ε^{P_r} , we obtain

$$\varepsilon^{P_r} r = \sum_{i=-1}^{N-1} a'_i \varepsilon^{-i+P_r} + \varepsilon^{-N} \sum_{j=0}^{\infty} (a_1 \varepsilon^{-(j-1)P_r} + a_2 \varepsilon^{-(j-1)P_r-1} + \dots + a_{P_r} \varepsilon^{-(j-1)P_r-P_r+1}).$$

Reindexing (4.22), we get

$$r = \sum_{i=-1}^{N-1} a'_i \varepsilon^{-i} + \varepsilon^{-N} \sum_{j=1}^{\infty} (a_1 \varepsilon^{-(j-1)P_r} + a_2 \varepsilon^{-(j-1)P_r-1} + \dots + a_{P_r} \varepsilon^{-(j-1)P_r-P_r+1}).$$

And thus

$$\varepsilon^{P_r} r - r = \left(\sum_{i=-1}^{N-1} a'_i \varepsilon^{-i+P_r} - a'_i \varepsilon^{-i} \right) + \varepsilon^{-N} (a_1 \varepsilon^{P_r} + a_2 \varepsilon^{P_r-1} + \dots + a_{P_r} \varepsilon).$$

Let

$$\alpha = \sum_{i=-1}^{N-1} a'_i \varepsilon^{-i+P_r}, \quad \text{and} \quad \beta = - \sum_{i=-1}^{N-1} a'_i \varepsilon^{-i}, \quad \text{and} \quad \gamma = \varepsilon^{-N} (a_1 \varepsilon^{P_r} + a_2 \varepsilon^{P_r-1} + \dots + a_{P_r} \varepsilon).$$

Note that, because α , β , and γ have finite ε expansions, we have that $\alpha, \beta, \gamma \in \mathbb{Z}[\varepsilon]$, and thus

$$\alpha + \beta + \gamma = \varepsilon^{P_r} r - r \in \mathbb{Z}[\varepsilon].$$

By definition, we know that

$$\varepsilon^{P_r} * r = \varepsilon^{P_r} r + z$$

for some $z \in \mathbb{Z}[\varepsilon]$. Thus, using Lemmas 2.8 and 4.6, we have

$$\varepsilon^{P_r} * r - r - z = \varepsilon^{P_r} r - r \implies \pi(\varepsilon^{P_r} * r - r - z) = \pi(\varepsilon^{P_r} r - r) \implies (\varepsilon^{P_r} + p\mathcal{O}_F - 1)\pi(r) = 0.$$

Since F is a field in which $\pi(r) \neq 0$ since $r \notin \mathcal{O}_F$, we have that

$$\varepsilon^{P_r} - 1 + p\mathcal{O}_F = 0 \implies \varepsilon^{P_r} \equiv 1 \pmod{p\mathcal{O}_F}.$$

for any $r \in R - \mathcal{O}_F$. Recall that M is the multiplicative order of ε in $\mathcal{O}_F/p\mathcal{O}_F$, so we see that $M | P_r$.

Next, we show that $P_r | M$. Since both r and $\varepsilon * r$ have periodic base- ε expansions, we let N_1 represent the smallest integer such that the repeating part of the base- ε expansion of r begins in the ε^{-N_1} place. Similarly, let N_2 represent the smallest integer such that the repeating part of the base- ε expansion of $\varepsilon * r$ begins in the ε^{-N_2} place.

Let $S = \max(N_1, N_2)$ be the smallest integer such that the base- ε expansion of both r and $\varepsilon * r$ is periodic for all indices greater than S . Thus, the digits in the $\varepsilon^{-S}, \varepsilon^{-S-1}, \dots, \varepsilon^{-S-P_r}$ place of the base- ε expansion of r constitute a full period, and we let the ordered set

$$\{x_1, x_2, \dots, x_{P_r}\}$$

represent the period set of r . As shown in Proposition 4.3, the operation $\varepsilon * r$ shifts the digits within the repeating part of the base- ε of r to the left by one index. In other words, the period set of $\varepsilon * r$ is the ordered set

$$\{x_2, \dots, x_{P_r}, x_1\}.$$

Note that moving between the period set of r and the period set of $\varepsilon * r$ can be represented by applying the permutation

$$\tau = (1 \ 2 \ \dots \ P_r) \in S_{P_r}$$

to the period set of r . Additionally, we have that $r = \varepsilon^M * r$, so the period sets of r and $\varepsilon^M * r$ must be equal. Thus,

$$\tau^M \{x_1, x_2, \dots, x_{P_r}\} = \{x_1, x_2, \dots, x_{P_r}\},$$

which implies that τ^M is the identity permutation. Since the order of $\tau \in S_{P_r}$ is P_r , we have that $P_r | M$. So, we see that $P_r = M$. \square

In our final lemma before we prove Theorem 1.2, we show that for any nontrivial Shintani cycle, the sum of the coefficients r_1 and r_2 where $r = r_1 + r_2\varepsilon$ of all the elements r in the Shintani cycle is a constant. In fact, these coefficients sum to M .

Lemma 4.9. *For any $r \in R - \mathcal{O}_F$, let $r' := r'_1 + r'_2\varepsilon$. Then,*

$$\sum_{r' \in C_r} (r'_1 + r'_2) = M.$$

Proof. Let $\varepsilon^i * r := r_1(i) + r_2(i)\varepsilon$, so $r_1(i+1) + r_2(i+1)\varepsilon = \varepsilon * (r_1(i) + r_2(i)\varepsilon)$. Recall that

$$\varepsilon * (r_1(i) + r_2(i)\varepsilon) = (1 - r_2(i)) + \{r_1(i) + \text{Tr}_{F/\mathbb{Q}}(\varepsilon)r_2(i)\}\varepsilon$$

by Lemma 4.4. Comparing coefficients, we see that $r_1(i+1) + r_2(i) = 1$ for all $i \in \mathbb{Z}$. Moreover, since $M = |C_r|$ for all $r \in R - \mathcal{O}_F$ by Lemma 4.7, we have that $r_1(m) = r_1(m+M)$ for any integer m . Using these facts, we see that

$$\begin{aligned} \sum_{r \in C_r} (r_1(i) + r_2(i)) &= \sum_{i=1}^M (r_1(i) + r_2(i)) = r_1(1) + r_2(M) + \sum_{i=1}^{M-1} r_1(i+1) + \sum_{j=1}^{M-1} r_2(j) \\ &= r_1(M+1) + r_2(M) + \sum_{i=1}^{M-1} (r_1(i+1) + r_2(i)) = 1 + (M-1) = M. \end{aligned}$$

\square

4.C. Proof of Theorem 1.2

Since $\langle \varepsilon \rangle$ acts on R , R decomposes into a disjoint union of Shintani cycles, under this action. Letting \mathcal{L} denote a complete reduced set of Shintani cycle representatives for R , and recalling that C_r denotes the Shintani cycle of r , we can rewrite Shintani's formula as follows:

$$\begin{aligned} h_K &= \frac{1}{2} \sum_{r \in R} \chi_{K/F}(rp\mathcal{O}_F) \sum_{\substack{0 \leq l_1, l_2 \leq 2 \\ l_1 + l_2 = 2}} \frac{B_{l_1}(r_1)}{l_1!} \frac{B_{l_2}(r_2)}{l_2!} \text{Tr}_{F/\mathbb{Q}}(\varepsilon)^{l_2-1} \\ &= \frac{1}{2} \sum_{i=1}^{|C_r|} \sum_{r \in \mathcal{L}} \chi_{K/F}(\varepsilon_F^i * r \cdot p\mathcal{O}_F) \sum_{\substack{0 \leq l_1, l_2 \leq 2 \\ l_1 + l_2 = 2}} \frac{B_{l_1}(r_1)}{l_1!} \frac{B_{l_2}(r_2)}{l_2!} \text{Tr}_{F/\mathbb{Q}}(\varepsilon)^{l_2-1} \end{aligned} \quad (4.23)$$

First, we show that $\chi_{K/F}(r' \cdot p\mathcal{O}_F)$ is constant for all $r' \in C_r$. By definition of $\varepsilon * r$, we see that $\varepsilon * r = \varepsilon r + z$ for some $z \in \mathcal{O}_F$. Thus

$$\chi_{K/F}(\varepsilon^i * r \cdot p\mathcal{O}_F) = \chi_{K/F}((\varepsilon^i r + z) \cdot p\mathcal{O}_F) = \chi_{K/F}(\varepsilon^i r p\mathcal{O}_F + z p\mathcal{O}_F).$$

Since $z p\mathcal{O}_F \subset p\mathcal{O}_F$, $p\mathcal{O}_F | z p\mathcal{O}_F$, and since $p\mathcal{O}_F$ is the conductor of this Hecke character, we see that

$$\chi_{K/F}(\varepsilon^i * r \cdot p\mathcal{O}_F) = \chi_{K/F}(\varepsilon^i r p\mathcal{O}_F).$$

Additionally, ε is a unit, so we know

$$r\mathcal{O}_F = \varepsilon^i r\mathcal{O}_F$$

for any integer i . Therefore

$$\chi_{K/F}(\varepsilon^i * r \cdot p\mathcal{O}_F) = \chi_{K/F}(\varepsilon^i r p\mathcal{O}_F) = \chi_{K/F}(r p\mathcal{O}_F),$$

and thus the Hecke character value in (4.23) is constant throughout each Shintani cycle.

By Lemma 4.7, all nontrivial Shintani cycles in R contain the same number of elements. Since $1/p$ is an element of $R - \mathcal{O}_F$ by Lemma 4.8, the period length $\ell_{F,p}$ of the base- ε expansion of $1/p$ is equal to the length of each nontrivial cycle.

Remark. Note that, for all $r \in R \cap \mathcal{O}_F$, the Hecke character $\chi_{K/F}(r p\mathcal{O}_F)$ evaluates to 0, so elements $r \in R \cap \mathcal{O}_F$ are all weighted by a factor of 0 in (4.23). Hence, we can ignore them in our calculations.

Using these facts, we obtain

$$h_K = \frac{1}{2} \sum_{i=1}^{\ell_{F,p}} \sum_{r \in \mathcal{L}} \chi_{K/F}(r p\mathcal{O}_F) \sum_{\substack{0 \leq l_1, l_2 \leq 2 \\ l_1 + l_2 = 2}} \frac{B_{l_1}(r_1) B_{l_2}(r_2)}{l_1! l_2!} \text{Tr}_{F/\mathbb{Q}}(\varepsilon)^{l_2 - 1}. \quad (4.24)$$

As shown in [BMT21], we have that

$$\sum_{r \in R} \chi_{K/F}(r p\mathcal{O}_F) = \sum_{r \in R \cap \mathcal{O}_F} \chi_{K/F}(r p\mathcal{O}_F) + \sum_{r \in R - \mathcal{O}_F} \chi_{K/F}(r p\mathcal{O}_F) = 0.$$

For all $r \in \mathcal{O}_F$, we have already seen that $\chi_{K/F}(r p\mathcal{O}_F) = 0$. Thus,

$$0 = \sum_{r \in R - \mathcal{O}_F} \chi_{K/F}(r p\mathcal{O}_F) = \sum_{r \in \mathcal{L} - \mathcal{O}_F} \chi_{K/F}(r p\mathcal{O}_F) \cdot \ell_{F,p} = \ell_{F,p} \sum_{r \in \mathcal{L} - \mathcal{O}_F} \chi_{K/F}(r p\mathcal{O}_F),$$

which yields

$$\sum_{r \in \mathcal{L} - \mathcal{O}_F} \chi_{K/F}(r p\mathcal{O}_F) = 0.$$

In other words, we have character orthogonality across the elements $r \in \mathcal{L} - \mathcal{O}_F$. With this, we consider the sum over Bernoulli polynomials within this formula. Letting

$$\mathcal{B}(r_1 + r_2 \varepsilon) := \sum_{\substack{0 \leq l_1, l_2 \leq 2 \\ l_1 + l_2 = 2}} \frac{B_{l_1}(r_1) B_{l_2}(r_2)}{l_1! l_2!} \text{Tr}_{F/\mathbb{Q}}(\varepsilon)^{l_2 - 1},$$

we see that

$$\begin{aligned} \mathcal{B}(r_1 + r_2 \varepsilon) &= \frac{r_1^2 - r_1 + \frac{1}{6}}{2} \text{Tr}_{F/\mathbb{Q}}(\varepsilon) + 2 \left(r_1 - \frac{1}{2} \right) \left(r_2 - \frac{1}{2} \right) + \frac{r_2^2 - r_2 + \frac{1}{6}}{2} \text{Tr}_{F/\mathbb{Q}}(\varepsilon) \\ &= \frac{\text{Tr}_{F/\mathbb{Q}}(\varepsilon)}{2} \left(r_1^2 + r_2^2 - (r_1 + r_2) + \frac{1}{3} \right) + 2r_1 r_2 - (r_1 + r_2) + \frac{1}{2}. \end{aligned} \quad (4.25)$$

Recall that by Lemmas 4.9, for all $r \in \mathcal{L} - \mathcal{O}_F$,

$$\sum_{r' \in C_r} r'_1 + r'_2 = M.$$

Thus, we can further simplify (4.25) to

$$\mathcal{B}(r_1 + r_2\varepsilon) = \frac{\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon)}{2} \left(r_1^2 + r_2^2 - M + \frac{1}{3} \right) + 2r_1r_2 - M - \frac{1}{2}. \quad (4.26)$$

Because we have character orthogonality over $\mathcal{L} - \mathcal{O}_F$, we can add a constant to the inner Bernoulli sum of (4.24) without changing the value of the whole expression. In particular, if we let

$$c := \frac{\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon)}{2} \left(-M + \frac{1}{3} \right) - M - \frac{1}{2},$$

we see that (4.26) can be rewritten as

$$\begin{aligned} \mathcal{B}(r_1 + r_2\varepsilon) &= \frac{\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon)}{2} \left(r_1^2 + r_2^2 \right) + 2r_1r_2 + c \\ &= \frac{1}{2} \left(\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon)r_1^2 + 4r_1r_2 + \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon)r_2^2 \right) + c. \end{aligned}$$

Using these results and letting $\varepsilon * r := r_1(i) + r_2(i)\varepsilon$, we obtain

$$h_K = \frac{1}{4} \sum_{i=1}^{\ell_{F,p}} \sum_{r \in \mathcal{L} - \mathcal{O}_F} \chi_{K/F}(rp\mathcal{O}_F) \left(\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon)r_1(i)^2 + 4r_1(i)r_2(i) + \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon)r_2(i)^2 \right).$$

Recall that $Q_F(Y_1, Y_2) := \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon)Y_1^2 + 4Y_1Y_2 + \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon)Y_2^2$. Thus if we make a slight abuse of notation by letting $Q_F(\varepsilon^i * r) = \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon)(r_1(i)^2 + 4r_1(i)r_2(i) + \mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon)r_2(i)^2)$, then we can express h_K as

$$h_K = \frac{1}{4} \sum_{i=1}^{\ell_{F,p}} \sum_{r \in \mathcal{L} - \mathcal{O}_F} \chi_{K/F}(rp\mathcal{O}_F) Q(\varepsilon^i * r).$$

5. Examples

Here we illustrate Theorems 1.1 and 1.2 for $\mathbb{Q}(\sqrt{3}, \sqrt{-p})$, where p is prime. Note that the ring of integers of $F = \mathbb{Q}(\sqrt{3})$ is given by $\mathbb{Z}[\sqrt{3}]$, and its totally positive unit group $\mathcal{O}_F^{\times,+}$ is generated by $\varepsilon_F = 2 + \sqrt{3}$. We require that $p \equiv 3 \pmod{4}$, $\left(\frac{3}{p}\right) = -1$, and $7 \leq p$. The first two conditions imply that the relative discriminant ideal is the prime ideal $p\mathbb{Z}[\sqrt{3}]$. Consequently, $\mathbb{Z}[\sqrt{3}]/p\mathbb{Z}[\sqrt{3}] \cong \mathbb{F}_p[\sqrt{3}]$.

5.A. Theorem 1.1 with $F = \mathbb{Q}(\sqrt{3})$

Let $\rho_{F,p} = a + b\sqrt{3}$ be a generator of $\mathbb{F}_p[\sqrt{3}]$. Table 1 lists values of $\rho_{F,p}$ as computed with SageMath. Using these values, we use (1.3) and (1.4) to calculate $C_{F,p}$ and $D_{F,p}$, then use (1.5) and (1.6) to find the corresponding rational functions $X_{F,p}(z)$ and $Y_{F,p}(z)$, which are also displayed in Table 1.

We extract the first $p^2 - 1$ coefficients from our rational functions by taking the k^{th} derivative of $X(z)$ and $Y(z)$, evaluating each function at $z = 0$, and dividing by $k!$. Note that in this case, since $t = 1$, we obtain only 1 sequence $x_1(m)$, and $y_1(m)$, from each of $X_{F,p}(z)$ and $Y_{F,p}(z)$ respectively. Since $\mathrm{Tr}_{F/\mathbb{Q}}(\varepsilon_F) = 4$, we have

$$Q_F(Y_1, Y_2) = 4Y_1^2 + 4Y_1Y_2 + 4Y_2^2.$$

Now we may apply Theorem 1.1 to obtain

$$h_{F(\sqrt{-p})} = \frac{1}{16p^2} \sum_{1 \leq m \leq p^2-1} (-1)^m Q_F(x_1(m), y_1(m)).$$

The smallest suitable prime for which we can apply Theorem 1.1 here is $p = 7$, for which we calculate

$$\begin{aligned} h_{F(\sqrt{-7})} &= \frac{1}{784} (-84 + 76 - 300 + 52 - 28 + 436 - 100 + 148 - 196 + 52 - 108 + 124 - 84 + 148 \\ &\quad - 36 + 172 - 28 + 124 - 12 + 76 - 196 + 172 - 4 + 156 - 84 + 76 - 300 + 52 - 28 \\ &\quad + 156 - 100 + 316 - 196 + 52 - 108 + 124 - 84 + 316 - 36 + 228 - 28 + 124 - 12 \\ &\quad + 76 - 196 + 228 - 4 + 436) = 2. \end{aligned}$$

In Table 1, we list some terms of our alternating sum for the class numbers of all such primes less than 100, along with the corresponding class numbers calculated using Theorem 1.1 and verified using SageMath.

p	$\rho_{F,p}$	$X_{F,p}(z)$	$Y_{F,p}(z)$	$h_{F(\sqrt{-p})}$ Calculation
7	$6 + \sqrt{3}$	$\frac{6z - 33z^2}{33z^2 - 12z + 1}$	$\frac{z}{33z^2 - 12z + 1}$	$\frac{1}{784} (-84 + 76 - \dots + 436) = 2$
19	$1 + 4\sqrt{3}$	$\frac{6z + 47z^2}{-47z^2 - 12z + 1}$	$\frac{4z}{-47z^2 - 12z + 1}$	$\frac{1}{5776} (-364 + 252 - \dots + 3892) = 2$
31	$1 + 6\sqrt{3}$	$\frac{z + 107z^2}{-107z^2 - 2z + 1}$	$\frac{6z}{-107z^2 - 2z + 1}$	$\frac{1}{15376} (-1084 + 676 - \dots + 10804) = 6$
43	$1 + 5\sqrt{3}$	$\frac{z + 74z^2}{-74z^2 - 2z + 1}$	$\frac{5z}{-74z^2 - 2z + 1}$	$\frac{1}{29584} (-3556 + 4836 - \dots + 21172) = 6$
67	$2 + 5\sqrt{3}$	$\frac{2z + 71z^2}{-71z^2 - 4z + 1}$	$\frac{5z}{-71z^2 - 4z + 1}$	$\frac{1}{71824} (-11772 + 2212 - \dots + 52276) = 6$
79	$2 + 6\sqrt{3}$	$\frac{2z + 104z^2}{-104z^2 - 4z + 1}$	$\frac{6z}{-104z^2 - 4z + 1}$	$\frac{1}{99856} (-16068 + 7372 - \dots + 73012) = 30$

Table 1: Theorem 1.1 for primes $p < 100$.

5.B. Theorem 1.2 with $F = \mathbb{Q}(\sqrt{3})$

We illustrate Theorem 1.2 in the same setting. Letting $F = \mathbb{Q}(\sqrt{3})$, we calculate h_K for $p \equiv 3 \pmod{4}$ where $7 \leq p$ and $\left(\frac{3}{p}\right) = -1$. We remind the reader that $\varepsilon_F = 2 + \sqrt{3}$, so $t = 1$. Thus by Lemma 2.9, $\ker(\pi) = R_{F,p} \cap \mathcal{O}_F = \{1\}$.

In the case that $p = 7$, we first calculate the base- ε_F expansion of $1/7$,

$$\begin{aligned} \frac{1}{7} &= \varepsilon_F^{-2} + 3\varepsilon_F^{-3} + 2\varepsilon_F^{-4} + 2\varepsilon_F^{-6} + 2\varepsilon_F^{-7} + 3\varepsilon_F^{-8} + 3\varepsilon_F^{-11} + 2\varepsilon_F^{-12} + 2\varepsilon_F^{-14} + 2\varepsilon_F^{-15} + 3\varepsilon_F^{-16} + \dots \\ &= 0.0132202230. \end{aligned}$$

Noticing that $1/7$ has period length $\ell_{F,7} = 8$, by Lemma 4.8, we can then deduce that there are

$$\frac{|R_{F,7} - \mathcal{O}_F|}{\ell_{F,7}} = \frac{1 \cdot 7^2 - 1}{8} = 6$$

disjoint Shintani cycles which comprise $R_{F,7} - \mathcal{O}_F$. We can generate these Shintani cycles explicitly, by calculating $\varepsilon_F^i * r$ for $0 \leq i < 8$ for $r \in R_{F,7} - \mathcal{O}_F$. One can verify that

$$\mathcal{L} = \left\{ \frac{1}{7} + \frac{1}{7}\varepsilon_F, \frac{1}{7}, \frac{1}{7} + \frac{4}{7}\varepsilon_F, \frac{1}{7} + \frac{5}{7}\varepsilon_F, \frac{2}{7} + \frac{2}{7}\varepsilon_F, \frac{3}{7} \right\}$$

is a complete reduced set of representatives for all 6 distinct nontrivial cycles in $R_{F,7}$. With these values, we now calculate $h_{F(\sqrt{-7})}$ using Theorem 1.2. Noting that $\text{Tr}_{F/\mathbb{Q}}(\varepsilon_F) = 4$ so $Q_F(Y_1, Y_2) = 4Y_1^2 + 4Y_1Y_2 + 4Y_2^2$, we compute

$$\begin{aligned} h_{F(\sqrt{-7})} &= \frac{1}{4} \sum_{i=1}^8 \sum_{r \in \mathcal{L}} \chi_{F(\sqrt{-7})/F}(rp\mathcal{O}_F) \left(4r_1(i)^2 + 4r_1(i)r_2(i) + 4r_2(i)^2 \right) \\ &= \frac{1}{4} \left(-\frac{220}{7} + \frac{228}{7} - \frac{188}{7} + \frac{212}{7} - \frac{180}{7} + \frac{204}{7} \right) = 2. \end{aligned}$$

In Table 2, we carry out the same procedure for all suitable primes less than 100.

p	Base ε_F Expansion of $1/p$	$\ell_{F,p}$	$h_{F(\sqrt{-p})}$ Calculation
7	0.01 $\overline{32202230}$	8	$\frac{1}{4} \left(-\frac{220}{7} + \frac{228}{7} - \frac{188}{7} + \frac{212}{7} - \frac{180}{7} + \frac{204}{7} \right) = 2$
19	0.002 $\overline{22231}$	5	$\frac{1}{4} \left(\frac{396}{19} + \frac{400}{19} - \frac{360}{19} + \dots + \frac{332}{19} + \frac{328}{19} \right) = 2$
31	0.001 $\overline{21320231203222210023032001222230}$	32	$\frac{1}{4} \left(\frac{3876}{31} - \frac{3788}{31} - \frac{3764}{31} - \dots - \frac{3444}{31} + \frac{3420}{31} \right) = 6$
43	0.001 $\overline{02311222230}$	11	$\frac{1}{4} \left(\frac{1856}{43} + \frac{1848}{43} + \frac{1940}{43} + \dots + \frac{1656}{43} + \frac{1624}{43} \right) = 6$
67	0.0002 $\overline{311001131322222132012210231222231}$	34	$\frac{1}{4} \left(\frac{8908}{67} + \frac{9228}{67} - \frac{8604}{67} + \dots + \frac{7492}{67} + \frac{7860}{67} \right) = 6$
79	0.0002 $\overline{122101031011213031211013010122113222220100121130211003030011203112100102222231}$	80	$\frac{1}{4} \left(\frac{22740}{79} - \frac{22364}{79} + \dots - \frac{22372}{79} + \frac{22500}{79} \right) = 30$

Table 2: Theorem 1.2 for primes $p < 100$.

Acknowledgements. The authors were participants in the 2023 UVA REU in Number Theory. They are grateful for the support of grants from Jane Street Capital, the National Science Foundation (DMS-2002265 and DMS-2147273), the National Security Agency (H98230-23-1-0016), and the Templeton World Charity Foundation. The authors thank Ken Ono, Wei-Lun Tsai, Alejandro De Las Penas Castano, and Eleanor McSpirit for suggesting the problem and for their mentorship and support. They would also like to thank Marie-Hélène Tomé and the other participants of the 2023 UVA REU for many thoughtful discussions. The authors would also like to thank the referee for their helpful comments on the manuscript.

References

- [BMT21] Adrian Barquero-Sanchez, Riad Masri, and Wei-Lun Tsai, Stark units and special gamma values. *Res. Number Theory* **7** 06 2021.
- [Cox89] David A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. 1989.
- [FrTa91] Albrecht Fröhlich and Martin J Taylor, *Algebraic Number Theory*, The Press Syndicate of Cambridge University, 1991.
- [Gir94] Kurt Girstmair, A “popular” class number formula, *Am. Math. Mon.* **101** 12 1994.
- [HaWr2008] G.H. Hardy, E.M. Wright, D.R. Heath-Brown, and J. Silverman, *An Introduction to the Theory of Numbers*, Oxford mathematics. 2008.
- [Hir87] Friedrich Hirzebruch, Hilbert modular surfaces and class numbers. *Gesammelte Abhandlungen*, 32-33:380–393, 1987.
- [Nar90] Wladyslaw Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 1990.
- [Neu11] Jürgen Neukirch, *Algebraic number theory*, Springer, 2011.
- [Sch80] Klaus Schmidt, On periodic expansions of pisot numbers and salem numbers, *Bull. Lond. Math. Soc.*, **12**(4) 269–278, 1980.
- [Shi76] Takuro Shintani, On evaluation of zeta functions of totally real algebraic number fields at non-positive integers, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, **23**(2) 393–417, 1976.
- [Zag75] Don Zagier, Nombres de classes et fractions continues, *Journées arithmétiques de Bordeaux, Astérisque*, **24-25** 81–97, 1975.

Elizabeth Athaide

Department of Mathematics, Massachusetts Institute of Technology
77 Massachusetts Avenue, Cambridge, MA 02139
e-mail: eathaide@mit.edu

Emma Cardwell

Department of Mathematics, Harvard University
1 Oxford Street, Cambridge, MA 02138
e-mail: ecardwell@college.harvard.edu

Christina Thompson

Department of Mathematics, Stanford University
450 Jane Stanford Way, Stanford, CA 94305
e-mail: cthomps@stanford.edu