DIVISIBILITY CRITERIA FOR CLASS NUMBERS OF IMAGINARY QUADRATIC FIELDS

PAUL JENKINS AND KEN ONO

ABSTRACT. In a recent paper, Guerzhoy obtained formulas for certain class numbers as p-adic limits of traces of singular moduli. Using earlier work by Bruinier and the second author, we derive a more precise form of these results using results of Zagier. Specifically, if $-d < -4$ is a fundamental discriminant and n is a positive integer, then

$$\mathrm{Tr}(p^{2n}d) \equiv \frac{24}{p-1} \cdot \left(1 - \left(\frac{-d}{p}\right)\right) \cdot H(-d) \pmod{p^n}$$

provided that $p \in \{2, 3\}$ and $\left(\frac{-d}{p}\right) = -1$, or $p \in \{5, 7, 13\}$ and $\left(\frac{-d}{p}\right) \neq 1$.

1. INTRODUCTION AND STATEMENT OF RESULTS

Throughout, let $d \equiv 0, 3 \pmod 4$ be a positive integer, and let $\mathcal{Q}_d$ denote the set of positive definite integral binary quadratic forms $Q(x, y) = ax^2 + bxy + cy^2 = [a, b, c]$ with discriminant $-d = b^2 - 4ac$ (including imprimitive forms if there are any). The group $\Gamma := \mathrm{PSL}_2(\mathbb{Z})$ acts on $\mathcal{Q}_d$ with finitely many orbits, and if ω_Q is defined by

$$\omega_Q = \begin{cases} 2 & \text{if } Q \sim_\Gamma [a, 0, a], \\ 3 & \text{if } Q \sim_\Gamma [a, a, a], \\ 1 & \text{otherwise,} \end{cases}$$

then the Hurwitz-Kronecker class number $H(-d)$ is given by

$$(1.1) \qquad H(d) = \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{1}{\omega_Q}.$$

If $-d < -4$ is a fundamental discriminant, then $H(-d)$ is the class number of the ring of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$.

Recently, Guerzhoy has obtained some interesting expressions for $\left(1 - \left(\frac{-d}{p}\right)\right) H(-d)$ as p-adic limits of traces of singular moduli. To make this precise, we first recall some notation. For positive definite binary quadratic forms Q, let α_Q be the unique root of

$Q(x, 1) = 0$ in the upper half of the complex plane. If $j(z)$ is the usual $\mathrm{SL}_2(\mathbb{Z})$ modular function

$$j(z) = \frac{E_4(z)^3}{\Delta(z)} = q^{-1} + 744 + 196884q + \cdots,$$

where $q = e^{2\pi i z}$, then define integers $\mathrm{Tr}(d)$ by

$$(1.2) \qquad \mathrm{Tr}(d) = \sum_{Q \in \mathcal{Q}_d/\Gamma} \frac{j(\alpha_Q) - 744}{\omega_Q}.$$

The algebraic integers $j(\alpha_Q)$ are known as *singular moduli*. Guerzhoy proved (see Corollary 2.4 (a) of [5]) that if $p \in \{3, 5, 7, 13\}$ and $-d < -4$ is a fundamental discriminant, then one has the p-adic limit formula

$$(1.3) \qquad \left(1 - \left(\frac{-d}{p}\right)\right) \cdot H(-d) = \frac{p-1}{24} \lim_{n \to +\infty} \mathrm{Tr}(p^{2n}d).$$

If $\left(\frac{-d}{p}\right) = 1$, then this result simply implies that $\mathrm{Tr}(p^{2n}d) \to 0$ p-adically as n tends to infinity. Thanks to work of Boylan, Edixhoven and the first author (see [2, 4, 6]), it turns out that more is true. In particular, if p is any prime and $\left(\frac{-d}{p}\right) = 1$, then

$$(1.4) \qquad \mathrm{Tr}(p^{2n}d) \equiv 0 \pmod{p^n}.$$

In earlier work [3], Bruinier and the second author obtained certain p-adic expansions for $H(-d)$ in terms of the Borcherds exponents of certain modular functions with Heegner divisor. In his paper [5], Guerzhoy asks whether there is a connection between (1.3) and these results when $\left(\frac{-d}{p}\right) \neq 1$. In this note we show that this is indeed the case by establishing the following congruences.

Theorem 1.1. *Suppose that $-d < -4$ is a fundamental discriminant and that n is a positive integer. If $p \in \{2, 3\}$ and $\left(\frac{-d}{p}\right) = -1$, or $p \in \{5, 7, 13\}$ and $\left(\frac{-d}{p}\right) \neq 1$, then*

$$\frac{24}{p-1} \cdot \left(1 - \left(\frac{-d}{p}\right)\right) \cdot H(-d) \equiv \mathrm{Tr}(p^{2n}d) \pmod{p^n}.$$

In particular, under these hypotheses p^n divides $\frac{24}{p-1}\left(1 - \left(\frac{-d}{p}\right)\right) \cdot H(-d)$ if and only if p^n divides $\mathrm{Tr}(p^{2n}d)$.

Three remarks.
1) Theorem 1.1 includes $p = 2$. For simplicity, Guerzhoy chose to work with odd primes p, and this explains the omission of $p = 2$ in (1.3).

2) Despite the uniformity of (1.4), it turns out that the restriction on p in Theorem 1.1 is required. For example, if $p = 11$, $n = 1$ and $-d = -15$, then $\left(\frac{-15}{11}\right) = -1$, $H(-15) = 2$,

and we have

$$\mathrm{Tr}(11^2 \cdot 15) = -13374447806956269126908865521582974841084501554961922745794$$

$$\equiv 7 \not\equiv \frac{48}{10} \cdot H(-15) \pmod{11}.$$

3) There are generalizations of Theorem 1.1 which hold for primes $p \notin \{2, 3, 5, 7, 13\}$. For example, one may employ Serre's theory [7] of p-adic modular forms to derive more precise versions of Corollary 2.4 (b) of [5].

2. The proof of Theorem 1.1

The proof of Theorem 1.1 follows by combining earlier work of Bruinier and the second author with results of Zagier and a combinatorial formula used earlier by the first author. We recall some necessary notation.

Let $M^!_{\lambda+\frac{1}{2}}$ be the space of weight $\lambda + \frac{1}{2}$ weakly holomorphic modular forms on $\Gamma_0(4)$ with Fourier expansion

$$f(z) = \sum_{(-1)^\lambda n \equiv 0,1 \pmod 4} a(n)q^n.$$

For $0 \leq d \equiv 0, 3 \pmod 4$, we let $f_d(z)$ be the unique form in $M^!_{\frac{1}{2}}$ with expansion

$$(2.1) \qquad f_d(z) = q^{-d} + \sum_{0 < D \equiv 0,1 \pmod 4} A(D, d)q^D.$$

The coefficients $A(D, d)$ of the f_d are integers. For completeness, we set $A(M, N) = 0$ if M or N is not an integer. These modular forms are described in detail in [8].

For fundamental discriminants $-d < -4$, Borcherds' theory on the infinite product expansion of modular forms with Heegner divisor [1] implies that

$$q^{-H(-d)} \prod_{n=1}^{\infty} (1 - q^n)^{A(n^2, d)}$$

is a weight zero modular function on $\mathrm{SL}_2(\mathbb{Z})$ whose divisor consists of a pole of order $H(-d)$ at infinity and a simple zero at each Heegner point of discriminant $-d$. Using this factorization, Bruinier and the second author proved the following theorem.

Theorem 2.1 ([3], Corollary 3). *Let $-d < -4$ be a fundamental discriminant. If $p \in \{2, 3\}$ and $\left(\frac{-d}{p}\right) = -1$, or $p \in \{5, 7, 13\}$ and $\left(\frac{-d}{p}\right) \neq 1$, then as p-adic numbers we have*

$$H(-d) = \frac{p-1}{24} \sum_{k=0}^{\infty} p^k A(p^{2k}, d).$$

Remark. The case when $p = 13$ is not proven in [3]. However, thanks to the remark preceding Theorem 8 of [7] on 13-adic modular forms with weight congruent to 2 (mod 12), and Theorem 2 of [3], the proof of Corollary 3 [3] still applies *mutatis mutandis.*

Zagier identified traces of singular moduli with the coefficients $A(D, d)$ as follows.

Theorem 2.2 ([8], Corollary to Theorem 3). *For all positive integers $d \equiv 0, 3$ (mod 4),*

$$\mathrm{Tr}(d) = A(1, d).$$

Combining Zagier's duality ([8], Theorem 4) between coefficients of modular forms in $M^!_{\frac{1}{2}}$ and in $M^!_{\frac{3}{2}}$ with the action of the Hecke operators on these spaces, the first author proved the following combinatorial formula.

Lemma 2.3 ([6], Theorem 1.1). *If p is a prime and d, D, n are positive integers such that $-d, D \equiv 0, 1$ (mod 4), then*

$$A(D, p^{2n}d) = p^n A(p^{2n}D, d) + \sum_{k=0}^{n-1} \left(\frac{D}{p}\right)^{n-k-1} \left(A\left(\frac{D}{p^2}, p^{2k}d\right) - p^{k+1} A\left(p^{2k}D, \frac{d}{p^2}\right) \right)$$

$$+ \sum_{k=0}^{n-1} \left(\frac{D}{p}\right)^{n-k-1} \left(\left(\left(\frac{D}{p}\right) - \left(\frac{-d}{p}\right) \right) p^k A(p^{2k}D, d) \right).$$

Remark. This result is stated for odd p in [6], but the proof holds for $p = 2$ as well.

Proof of Theorem 1.1. Under the given hypotheses, Theorem 2.1 implies that

$$(2.2) \qquad \frac{24}{p-1} \cdot H(-d) \equiv \sum_{k=0}^{n-1} p^k A(p^{2k}, d) \pmod{p^n}.$$

By letting $D = 1$ in Lemma 2.3, for these d and p we find that

$$(2.3) \qquad \left(1 - \left(\frac{-d}{p}\right)\right) \sum_{k=0}^{n-1} p^k A(p^{2k}, d) = A(1, p^{2n}d) - p^n A(p^{2n}, d).$$

Inserting this expression for the sum into (2.2), we conclude that

$$\frac{24}{p-1} \cdot \left(1 - \left(\frac{-d}{p}\right)\right) \cdot H(-d) \equiv A(1, p^{2n}d) \pmod{p^n},$$

which by Zagier's theorem is $\mathrm{Tr}(p^{2n}d)$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

References

[1] R. E. Borcherds, *Automorphic forms on $O_{s+2,2}(\mathbb{R})$ and infinite products*, Invent. Math. **120** (1995), no. 1, 161–213.

[2] M. Boylan, *2-adic properties of Hecke traces of singular moduli*, Math. Res. Lett. **12** (2005), no. 4, 593–609.

[3] J. H. Bruinier and K. Ono, *The arithmetic of Borcherds' exponents*, Math. Ann. **327** (2003), no. 2, 293–303.

[4] B. Edixhoven, *On the p-adic geometry of traces of singular moduli*, International Journal of Number Theory **1** (2005), 495–497.

[5] P. Guerzhoy, *The Borcherds-Zagier isomorphism and a p-adic version of the Kohnen-Shimura map*, Int. Math. Res. Not. (2005), no. 13, 799–814.

[6] P. Jenkins, *p-adic properties for traces of singular moduli*, International Journal of Number Theory **1** (2005), 103–107.

[7] J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), Springer, Berlin, 1973, pp. 191–268. Lecture Notes in Math., Vol. 350.

[8] D. Zagier, *Traces of singular moduli*, Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998), Int. Press Lect. Ser., vol. 3, Int. Press, Somerville, MA, 2002, pp. 211–244.

UCLA MATHEMATICS DEPARTMENT, LOS ANGELES, CALIFORNIA 90095-1555
E-mail address: jenkins@math.ucla.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, MADISON, WISCONSIN 53706
E-mail address: ono@math.wisc.edu