ZETA FUNCTIONS FOR IDEAL CLASSES IN REAL QUADRATIC FIELDS, AT $s = 0$.

András Biró and Andrew Granville

1. Introduction

Let K be a real quadratic field with discriminant d, and for a (fractional) ideal a of K, let Na be the norm of a. For a given fractional ideal I of K, and Dirichlet character χ of conductor q, we define

$$\zeta_I(s,\chi) = \zeta_{Cl(I)}(s,\chi) := \sum_a \frac{\chi(Na)}{(Na)^s}$$

where the sum is over all integral ideals of K which are equivalent to I. Our goal is to give a short (finite) formula to evaluate $\zeta_I(0,\chi)$.

Our starting point is the well known formula that, for the Dirichlet L-function $L(s,\chi)$, we have

$$L(0,\chi) = -\sum_{1\le a\le q-1} \chi(a)\ \frac{a}{q} \quad \text{whenever } \chi(-1) = -1, \tag{1}$$

which we wish to generalize to our new situation. We think of (1) as the one-dimensional case. To find the natural two-dimensional formula one must first realize that the set of rational integers which arise from considering K is not the set of all integers, but rather the set of norms of integral ideals of K. These can be expressed as the set of values taken by certain binary quadratic forms f of discriminant d, and this leads us to define

$$G(f,\chi) := \sum_{1\le m,n\le q-1} \chi(f(m,n))\ \frac{m}{q}\ \frac{n}{q}, \tag{2}$$

as a generalization of (1).

In order to relate $G(f,\chi)$ to $\zeta_I(0,\chi)$, we need to review the classical theory of cycles of reduced forms corresponding to a given ideal: For $\beta\in K$, write $\beta \gg 0$, and say that β is totally positive, if $\beta > 0$ and $\overline{\beta} > 0$, where $\overline{\beta}$ denotes the algebraic conjugate of β. Any ideal I of K has a $\mathbb{Z}$-basis (v_1, v_2) of I for which $v_1 \gg 0$ and such that if $\alpha = v_2/v_1$ then $0 < \alpha < 1$ and the regular continued fraction expansion of α is purely periodic, that is

$$\alpha = [0, \overline{a_1, \dots, a_\ell}]$$

for some positive integers ℓ and $a_1, \dots, a_\ell$, see Remark 1 below. Note that $a_{j+\ell} = a_j$ for all $j \geq 1$. For $n \geq 1$ we denote $p_n/q_n := [0, a_1, a_2, \dots, a_n]$ and we write $\alpha_n := p_n - q_n\alpha$ with $\alpha_{-1} = 1$ and $\alpha_0 = -\alpha$. Finally define

$$f_j(x,y) = (v_1\alpha_{j-1}x + v_1\alpha_j y)(\overline{v_1\alpha}_{j-1}x + \overline{v_1\alpha}_j y)/NI \qquad \text{for } j = 1, 2, \dots,$$

and

$$f_j(x,y) = (-1)^j Q_j(x,y).$$

Note that every Q_j has integer coefficients, and the discriminant of Q_j is

$$\left(\frac{v_1\overline{v_1}}{NI}\right)^2 (\alpha_{j-1}\overline{\alpha}_j - \overline{\alpha}_{j-1}\alpha_j)^2 = \left(\frac{v_1\overline{v_1}}{NI}\right)^2 (\alpha_{-1}\overline{\alpha}_0 - \overline{\alpha}_{-1}\alpha_0)^2 = \left(\frac{v_1\overline{v_1}(\alpha - \overline{\alpha})}{NI}\right)^2 = d.$$

It is easy to show that $\zeta_I(0,\chi) = 0$ if $\chi(-1) = 1$, so we again restrict ourselves to the case $\chi(-1) = -1$.

Theorem 1. *Suppose that χ is a primitive character mod $q > 1$ where $(q, 2d) = 1$ and $\chi(-1) = -1$. With the notations as above, we have*

$$\zeta_I(0,\chi)/2 = \sum_{j=1}^{\ell} G(f_j,\chi) + \frac{1}{2}\chi(d)\left(\frac{d}{q}\right)\beta_\chi \sum_{j=1}^{\ell} a_j \overline{\chi}(f_j(1,0)),$$

where $\beta_\chi := \chi(-1)\tau(\chi)^2 L(2,\overline{\chi}^2)/\pi^2$.

Here the Gauss sum $\tau(\psi) := \sum_{a \pmod q} \chi(a) e^{2i\pi a/q}$. The expression for β_χ involves an infinite product as well as a π^2, so is neither obviously algebraic nor computationally useful. However, using the functional equation for Dirichlet L-functions this can be rewritten as a simple finite expression: For χ primitive then there is a unique way to write $\chi = \chi_+\chi_-$ where χ_+, χ_- are primitive characters of coprime conductors q_+, q_- respectively such that χ_- has order 2, and χ_+^2 is also primitive. We then have $\beta_\chi = \frac{q}{6}\prod_{p|q}(1 - p^{-2})$ if χ has order 2, and

$$\beta_\chi = \chi_+(-1) J_{\chi_+} \gamma_\chi \ \mu(q_-) \prod_{p|q_-} \left(\frac{p^2\chi_+^2(p) - 1}{p\chi_+^2(p) - 1}\right) \text{ where } \gamma_\chi := \sum_{n=0}^{q-1} \chi^2(n)\frac{n^2}{q^2},$$

if χ has order > 2, where the Jacobi sum $J_\chi := \sum_{a,b \pmod q:\ a+b=1} \chi(a)\chi(b)$.

This formula in Theorem 1 is typically shorter, and arguably easier to compute, than those proposed by Shintani [5], Zagier [9], and Stark-Hayes [3]. This is not too surprising since we borrow ideas from all of these papers.

Remark 1. For a given ideal I, we can always choose a basis (v_1, v_2) with the stated properties. Indeed, starting from any basis, using the transformations

$$(v_1, v_2) \to (v_1, -v_2),\ (v_1, v_2) \to (v_2, v_1),\ (v_1, v_2) \to (v_1, v_2 - nv_1)$$

(where n is any rational integer) we can achieve that $v_1 > 0$ and $\alpha = v_2/v_1$ has a purely periodic continued fraction. If $\overline{v_1} > 0$, we are done. If $\overline{v_1} < 0$, then $v_2 \gg 0$, because $\overline{\alpha} < 0$ (by the Galois-Legendre theorem), in which case the basis $(v_2, v_1 - a_1 v_2)$ has the required properties.

1b. Other special values of $\zeta_I(s,\chi)$. In order to generalize (1) and Theorem 1 to $\zeta_I(1-k,\chi)$ for $k \geq 1$, it will pay to slightly reformulate the above results, simply by replacing a/q in (1) by $a/q - 1/2$, and similarly m/q and n/q in (2). This new polynomial $t - 1/2$ is the first Bernoulli polynomial. The Bernoulli polynomials can be defined by the generating function

$$\text{(3)} \qquad \frac{Te^{Tx}}{e^T - 1} = \sum_{n\geq 0} B_n(x)\frac{T^n}{n!};$$

note that $B_n(1-x) = (-1)^n B_n(x)$ by definition. The Bernoulli numbers are given by $B_n = B_n(0)$ and then $B_n(x) = \sum_{0\leq i\leq n}\binom{n}{i}B_i x^{n-i}$. It is well-known that for any primitive $\chi \pmod q$ with $q > 1$, we have

$$\text{(4)} \qquad L(1-k,\chi) = -\frac{q^{k-1}}{k}\sum_{1\leq a\leq q-1}\chi(a)B_k(a/q).$$

(Note that $\gamma_\chi = -2L(-1,\chi^2)/q$ if χ has order > 2.) We prove an analogous result for $\zeta_I(1-k,\chi)$. First define the functions $p_{r,s}(x,y)$ where r,s are positive integers with $r+s = 2k$, and $x,y \in K$,

$$p_{r,s}(x,y) := \frac{1}{r!}\frac{1}{s!}\sum_{\substack{h,i\in\mathbb{Z}\\ h+i=k-1}}\binom{r-1}{h}\binom{s-1}{i}x^h\overline{x}^{r-1-h}y^i\overline{y}^{s-1-i},$$

(where $\binom{-1}{i} = \frac{1}{2}(-1)^i$ if $i \geq 0$, and $\binom{-1}{i} = -\frac{1}{2}(-1)^i$ if $i < 0$); and, in analogy to (2),

$$G_{r,s}(f,\chi) := \sum_{0\leq m,n\leq q-1}\chi(f(m,n))B_r\left(\frac{m}{q}\right)B_s\left(\frac{n}{q}\right).$$

It can be shown that if $\chi(-1) = (-1)^{k-1}$ then $\zeta_I(1-k,\chi) = 0$, so we restrict ourselves to the case $\chi(-1) = (-1)^k$.

Theorem 2. *For any $k \geq 1$ and for any primitive $\chi \pmod q$ with $q > 1$ where $(q,d) = 1$ and $\chi(-1) = (-1)^k$, we have*

$$\zeta_I(1-k,\chi) = 2\left(\frac{q^2 v_1\overline{v_1}}{NI}\right)^{k-1}(k-1)!^2\sum_{j=1}^{\ell}(-1)^j\sum_{\substack{r,s\geq 0\\ r+s=2k}}p_{r,s}(\alpha_{j-1},\alpha_j)G_{r,s}(Q_j,\chi).$$

1c. Speculative generalization. The results in Theorems 1 and 2 beg to be generalized, to further extensions of $\mathbb{Q}$: Now let K be a number field (perhaps one should assume that $K/\mathbb{Q}$ is an abelian extension) of degree D, and let I be an integral ideal of K. We define $\zeta_I(s,\chi)$ as above. We may associate to I a finite set of norm forms $f_1, f_2, \dots, f_\ell \in \mathbb{Z}[X_1,\dots,X_D]$ each of degree $\leq D$: typically these are the norms for $K/\mathbb{Q}$ of algebraic integers of the form $X_1\omega_1 + X_2\omega_2 + \cdots + X_D\omega_D$, where $\{\omega_1,\omega_2,\dots,\omega_D\}$ forms a $\mathbb{Z}$-basis for I. Here $\ell = \ell(I)$ and the set of forms depend only on the ideal class of I. Now to each f_j we may associate a finite set of integers S_j as well as particular integers a_j, b_j. We guess that if $\chi(-1) = -1$ then $\zeta_I(0,\chi)$ equals

$$\sum_{j=1}^{\ell} \sum_{1\leq m_1,\dots,m_D\leq q-1} \chi(f_j(m_1,\dots,m_D))g_D\left(\frac{m_1}{q},\dots,\frac{m_D}{q}\right) + \beta_{\chi,D}\sum_{j=1}^{\ell} a_j \sum_{n_j\in S_j} \overline{\chi}(n_j)$$

for some homogenous form $g_D(X_1,\dots,X_D)$ of degree D which is independent of K, and certain easily described algebraic integers $\beta_{\chi,D}$, also independent of K.

Note that theorem 1 is a special case of this taking $g_2(X,Y) = 2XY$, $S_j = \{f_j(1,0)\}$ and $\beta_{\chi,2} = 2\beta_\chi$.

These speculations complement, in some sense, the much deeper conjectures made by Stark [7]. In Stark's conjecture the value of the L-function is given in term of a unit and is thus "basis-independent", something which our speculations are not. A more geometric formulation is to think of $G(f,\chi)$ as the discrete analogue of the integral of a continuous function of f, on the unit square. In other words if H is a function of one variable then one can consider the integrals

$$\int_{t=0}^{1} H(t)t \, \mathrm{d}t \quad \text{and} \quad \int_{t=0}^{1}\int_{u=0}^{1} H(f(t,u))tu \, \mathrm{d}u \, \mathrm{d}t$$

where f is homogenous. The q-analogue of these are where we take $H(x) = \chi(q^d x), t = m/q, u = n/q$ (with $d = 1,2$ respectively), and replace the integrals by the sum over those points (t,u) for which $qt, qu \in \mathbb{Z}$, obtaining the functions in (1) and (2)!

Can we check this conjecture in $\mathbb{Q}(\zeta_5)$?

1d. Small class numbers and fundamental unit. In [1,2] Biró determined the complete list of d of the forms n^2+4 and $4n^2+1$ such that $\mathbb{Q}(\sqrt{d})$ has class number one, so resolving the Yokoi and Chowla conjectures, respectively. Notice that the fundamental unit $\epsilon_d = (u_d + v_d\sqrt{d})/2$ with $u_d, v_d > 0$ satisfies $|\epsilon_d - v_d\sqrt{d}| \leq 3/v_d\sqrt{d}$, so that ϵ_d is very close to an integer multiple of $\sqrt{d}$. Therefore the smallest ϵ_d can be as a function of d, is close to $1\times\sqrt{d}$, that is $v_d = 1$, in which case $d = u^2 \pm 4$, and one can evidently only have class number one if d is prime, whence d must be of the form n^2+4. If $v_d = 2$ and d is prime then $u = 4n$ for some integer n and thus d must be of the form $4n^2+1$. Now, Dirichlet's class number formula tells us that $h(d)\log\epsilon_d = \pi\sqrt{d}L(1,(./d))$, so if $h(d) = 1$ and ϵ_d is no bigger than some fixed multiple of $\sqrt{d}$ then we deduce that $L(1,(./d)) \ll \log d/\sqrt{d}$. This only happens for finitely many d, by the ineffective Siegel's theorem. A variant of

Siegel's theorem, due to Tatuzawa, allows one to easily determine all d with $h(d) = 1$ and $\epsilon_d \ll \sqrt{d}$, with at most one possible exception: one does not expect that there are any exceptions but the proof does not permit one to check this. Even the much celebrated lower bounds of Goldfeld, Gross and Zagier, do not help with this problem, so the results of [1,2] overcame what had been longstanding open problems.

Our Theorem 1 extends the formulae of [1,2], allowing us to check those results and to extend them somewhat.

2. Notation

Let $I_F(K)$ be the set of nonzero fractional ideals of K, and let $P_F(K)$ be the set of nonzero principal fractional ideals of K.

If $I_1, I_2 \in I_F(K)$, we say that they are relatively prime and write $(I_1, I_2) = 1$, if expressing the fractional ideals as quotients of relatively prime integral ideals: $I_1 = a_1 b_1^{-1}$, $I_2 = a_2 b_2^{-1}$, the integral ideals $a_1 b_1$ and $a_2 b_2$ are relatively prime.

For $\beta \in K$ let $\mathrm{Tr}(\beta) = \beta + \overline{\beta}$. If q is a positive rational integer and $\beta_1, \beta_2 \in K$, we write $\beta_1 \equiv \beta_2 \pmod q$ if there exists a rational integer n with $(n, q) = 1$ such that $n(\beta_1 - \beta_2)/q$ is an algebraic integer.

Let $0 < \epsilon_+ < 1$ be a fundamental totally positive unit, let m be the smallest positive integer such that $\epsilon_+^m \equiv 1 \pmod q$.

Let $I \in I_F(K)$, and assume that (v_1, v_2) is a $\mathbb{Z}$-basis of I for which $v_1 \gg 0$ and such that $\alpha = v_2/v_1$ where $0 < \alpha < 1$ and the regular continued fraction expansion of α is purely periodic. We have $\epsilon_+ \alpha_r = \alpha_{L+r}$ for $r \geq -1$, in particular $\epsilon_+ = \alpha_{L-1}$, $\epsilon_+^m = \alpha_{Lm-1}$. It is clear that $(v_1 \alpha_{j-1}, v_1 \alpha_j)$ is a basis of I for any $j \geq 0$.

Let $(N)_q$ denote the least nonnegative residue of N modulo q. Let $\lceil t \rceil$ denote the least integer not smaller than t.

Now, if $v \in I$, then C_j, D_j are selected to be those unique rational integers that satisfy

$$C_j v_1 \alpha_{j-1} + D_j v_1 \alpha_j = v \qquad \text{for all } \; j \geq 0;$$

and then we denote $c_j = (C_j)_q/q$ and $d_j = (D_j)_q/q$. It is clear that $c_{j+Lm} = c_j$, $d_{j+Lm} = d_j$. If we want to denote the dependence on v, we write $C_j(v), D_j(v), c_j(v), d_j(v)$. Note that since $\epsilon_+ \alpha_j = \alpha_{j+L}$ we deduce from the definition that $C_{j+L}(v\epsilon_+) = C_j(v)$ and $D_{j+L}(v\epsilon_+) = D_j(v)$.

It is a simple matter to establish, using the recursion formula $\alpha_{j-2} + a_j \alpha_{j-1} = \alpha_j$ for each $j \geq 1$, to show that

$$D_{j+1} = C_j \text{ and } C_{j+1} = D_j - a_{j+1} C_j \qquad \text{for all } \; j \geq 0. \tag{2.3}$$

Therefore $a_{j+1} c_j - d_j + c_{j+1}$ is an integer and $0 \leq c_{j+1} < 1$, so that

$$\lceil a_{j+1} c_j - d_j \rceil = a_{j+1} c_j - d_j + c_{j+1} = a_{j+1} c_j - c_{j-1} + c_{j+1}. \tag{2.4}$$

3. Evaluating a sectorial zeta function

Let $I \in I_F(K)$, $v \in I$, let q be a positive rational integer such that $(v,q)=(I,q)=1$ (where we write v and q for the principal fractional ideals generated by these elements), and define

$$\zeta_{I,v,q}(s) = \sum_{a \in P_{I,v,q}} (Na)^{-s},$$

where $P_{I,v,q} = \{a \in P_F(K) : a = (\beta) \text{ for some } \beta \in I,\ \beta \equiv v \pmod q,\ \beta \gg 0\}$.

Theorem 3.1. *If $(v,q)=(I,q)=1$ then*

$$\zeta_{I,v,q}(0) = \sum_{j=0}^{Lm-1} (-1)^j \left(\frac{a_j}{2} B_2(d_j) + c_j d_j \right)$$

Our proof of this theorem is based, first of all, on Shintani's method, but to get this simple form, we use ideas from [3] and [1]. The most important idea used here from [3] (which, as Hayes writes, goes back to [9]) is (in the language of [3]) subdividing the fundamental domain into sectors before applying Shintani's method. (In our language this means that we write the set $Q_{I,v,q}^{(v_1, v_1 \epsilon_+^m)}$ below as a disjoint union of smaller sets.) However, we subdivide the set into fewer parts (using the regular continued fraction expansion instead of the type II continued fractions) than it is done in [3]. Inside a given part, we can give a simple formula (see Corollary 4.2 below) for the value at 0 by generalizing the proof of Lemma 1 of [1]. In the case of the special fields and principal I considered in [1], essentially one application of our present Corollary 4.2 led to the final result, here we have to apply this corollary several times. It is likely that our formula could be also derived from the CF-formula of [3] by summing over collinear vertices of the convexity polygon; this summation step would then correspond to our Corollary 4.2.

If q is fixed and we vary the field K, our formula consists of fewer terms than the CF-formula of [3]: the CF-formula in this case has around $a_1 + a_2 + \ldots + a_L$ terms, while our formula has $O(L)$ terms. So, if q and L are fixed, our formula has a bounded number of terms, which fact was very important in the proofs in [1,2].

4. Shintani's theorem

For a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with positive entries and $x > 0$, $y \geq 0$, define

$$\zeta\left(s, \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (x,y)\right) := \sum_{n_1,n_2=0}^{\infty} \left(a(n_1+x) + b(n_2+y)\right)^{-s} \left(c(n_1+x) + d(n_2+y)\right)^{-s}.$$

The Corollary to Proposition 1 of [5] implies the following:

Proposition 4.1. (Shintani). *For any $a, b, c, d, x > 0$ and $y \geq 0$ the function*

$$\zeta\left(s, \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (x, y)\right),$$

is absolutely convergent for $\Re s > 1$, extends meromorphically in s to the whole complex plane, and

$$\zeta\left(0, \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (x, y)\right) = B_1(x)B_1(y) + \frac{1}{4}\left(B_2(x)\left(\frac{c}{d} + \frac{a}{b}\right) + B_2(y)\left(\frac{d}{c} + \frac{b}{a}\right)\right).$$

The Bernoulli polynomials $B_\ell(t)$ have the remarkable property that

$$\sum_{j=0}^{k-1} B_\ell\left(t + \frac{j}{k}\right) = k^{-(\ell-1)} B_\ell(kt). \tag{4.1}$$

We deduce the following:

Corollary 4.2. *Let (e, f) be a basis of I, t a positive integer, $e^* = e + tf$, and assume that $e, e^* \gg 0$. Furthermore, let $w = Ce + Df$ with some rational integers $0 \leq C, D < q$, and write $c = \frac{C}{q}$, $d = \frac{D}{q}$, $\delta = \frac{(D-tC)_q}{q}$. Let*

$$Z(s) = \sum_{\beta \in H} (\beta\overline{\beta})^{-s}$$

with $H = \{\beta \in I : \beta \equiv w \pmod{q}, \beta = Xe + Ye^* \text{ with } (X, Y) \in \mathbb{Q}^2,\ X > 0,\ Y \geq 0\}$. Then

$$Z(0) = A(1 - c) + \frac{t}{2}\left(c^2 - c - \frac{1}{6}\right) + \frac{d - \delta}{2} + \mathrm{Tr}\left(\frac{-f}{4e^*}\right) B_2(\delta) + \mathrm{Tr}\left(\frac{f}{4e}\right) B_2(d),$$

where $A = \lceil tc - d \rceil$.

Proof. Note that $A = \lceil \frac{tC-D}{q} \rceil = \frac{tC-D+q\delta}{q} = tc - d + \delta$ and therefore $0 \leq A \leq t$. Let $\beta = Xe + Ye^*$ for some rationals $X > 0$, $Y \geq 0$. Write $X = qx + qn_1$ and $Y = qy + qn_2$ for some nonnegative integers n_1 and n_2 and rational numbers $0 < x \leq 1$, $0 \leq y < 1$ which can be done in a unique way. Then, on the one hand,

$$\beta\overline{\beta} = q^2\left(e(n_1 + x) + e^*(n_2 + y)\right)\left(\overline{e}(n_1 + x) + \overline{e^*}(n_2 + y)\right);$$

on the other hand we have that $\beta \in I$ and $\beta \equiv w \pmod{q}$ hold if and only if $xe + ye^* - (ce + df) \in I$. Therefore

$$Z(s) = \frac{1}{q^{2s}} \sum_{(x,y) \in R(C,D)} \zeta\left(s, \begin{pmatrix} e & e^* \\ \overline{e} & \overline{e^*} \end{pmatrix}, (x, y)\right)$$

where $R(C,D) := \{(x,y) \in \mathbb{Q}^2 :\ 0 < x \le 1,\ 0 \le y < 1,\ xe + ye^* - (ce+df) \in I\}$. Therefore by Proposition 4.1 we get

$$Z(0) = \sum_{(x,y)\in R(C,D)} \left(B_1(x)B_1(y) + \mathrm{Tr}\left(\frac{e}{4e^*}\right) B_2(x) + \mathrm{Tr}\left(\frac{e^*}{4e}\right) B_2(y) \right).$$

We observe that for any m, n we have

$$\frac{mf+ne}{q} = \frac{(n-\frac{m}{t})e + \frac{m}{t}e^*}{q},$$

and so it is easy to see that the possibilities for (m,n) having $(x,y) \in R(C,D)$ with

$$(x,y) = \left(\frac{1}{q}\left(n - \frac{m}{t}\right), \frac{1}{q}\frac{m}{t} \right)$$

are

$$m_j = D + jq, \quad n_j = C + q\left\lfloor 1 + \frac{j}{t} - \frac{(tC-D)/q}{t} \right\rfloor$$

with any integer $0 \le j \le t-1$. This is so because the possible values of m are obviously these t values, and once m is fixed, n is unique. Now

$$0 < 1 + \frac{j}{t} - \frac{(tC-D)/q}{t} < 2, \quad \text{so} \quad n_j = \begin{cases} C & \text{if } 0 \le j < A \\ C+q & \text{if } A \le j < t \end{cases},$$

and therefore

$$Z(0) = \sum_{j=0}^{t-1} \left(B_1(x_j)B_1(y_j) + \mathrm{Tr}\left(\frac{e}{4e^*}\right) B_2(x_j) + \mathrm{Tr}\left(\frac{e^*}{4e}\right) B_2(y_j) \right)$$

$$\text{where} \quad y_j = \frac{d+j}{t} \ \text{for } 0 \le j < t, \ \text{and } x_j = \begin{cases} c - y_j & \text{if } 0 \le j < A; \\ c+1-y_j & \text{if } A \le j < t. \end{cases}$$

Now, by (4.1) we have

$$\sum_{j=0}^{t-1} B_2(y_j) = \sum_{j=0}^{t-1} B_2\left(\frac{d+j}{t}\right) = \frac{1}{t}B_2(d);$$

and

$$\sum_{j=0}^{t-1} B_2(x_j) = \sum_{j=0}^{A-1} B_2\left(\frac{A-j-\delta}{t}\right) + \sum_{j=A}^{t-1} B_2\left(\frac{t+A-j-\delta}{t}\right)$$
$$= \sum_{k=1}^{t} B_2\left(\frac{k-\delta}{t}\right) = \sum_{l=0}^{t-1} B_2\left(\frac{\delta+l}{t}\right) = \frac{1}{t}B_2(\delta).$$

Now since $B_2(x) + B_2(y) + 2B_1(x)B_1(y) = (x + y - 1)^2 - \frac{1}{6}$ we easily deduce that

$$\sum_{j=0}^{t-1}(B_2(x_j) + B_2(y_j) + 2B_1(x_j)B_1(y_j)) = A(c-1)^2 + (t-A)c^2 - \frac{t}{6}.$$

The result then follows from the last four displayed equations, and the facts that

$$\mathrm{Tr}\left(\frac{e}{4te^*}\right) - \frac{1}{2t} = \mathrm{Tr}\left(\frac{-f}{4e^*}\right) \text{ and } \mathrm{Tr}\left(\frac{e^*}{4te}\right) - \frac{1}{2t} = \mathrm{Tr}\left(\frac{f}{4e}\right).$$

5. Special value of the sectorial zeta function

Proof of Theorem 3.1. If $a \in P_{I,v,q}$ and $a = (\beta)$ for some $\beta \in I, \beta \equiv v \pmod{q}$, $\beta \gg 0$ then, since $(v, q) = (I, q) = 1$, the generators of a with these properties are precisely the numbers $\beta(\epsilon_+^m)^j$ for any integer j. Therefore,

$$\zeta_{I,v,q}(s) = \zeta_{I,v,q}^{(v_1, v_1\epsilon_+^m)}(s) \text{ where } \zeta_{I,v,q}^{(\beta_1,\beta_2)}(s) := \sum_{\beta}(\beta\overline{\beta})^{-s},$$

the sum over $\beta \in Q_{I,v,q}^{(\beta_1,\beta_2)} = \left\{\beta \in I : \beta \equiv v \pmod{q},\ \beta \gg 0,\ \beta_2/\overline{\beta_2} < \beta/\overline{\beta} \le \beta_1/\overline{\beta_1}\right\}$, for any given $\beta_1, \beta_2 \in K$, $\beta_1, \beta_2 \gg 0$.

Since $\overline{\alpha} < 0$ and $v_1 \gg 0$ we deduce that $v_1\alpha_{-1} > v_1\alpha_1 > v_1\alpha_3 > \ldots > 0$, and $0 < \overline{v_1\alpha_{-1}} < \overline{v_1\alpha_1} < \overline{v_1\alpha_3} < \ldots$, so that $v_1\alpha_{-1}/\overline{v_1\alpha_{-1}} > v_1\alpha_1/\overline{v_1\alpha_1} > v_1\alpha_3/\overline{v_1\alpha_3} > \ldots > 0$. Recalling that $\epsilon_+^m = \alpha_{2lm-1}$, we deduce that $Q_{I,v,q}^{(v_1,v_1\epsilon_+^m)}$ is the disjoint union of the sets

$$Q_{I,v,q}^{(v_1\alpha_{2r-1}, v_1\alpha_{2r+1})} \text{ for } 0 \le r < lm$$

so that

$$\zeta_{I,v,q}(s) = \sum_{r=0}^{lm-1} \zeta_{I,v,q}^{(v_1\alpha_{2r-1}, v_1\alpha_{2r+1})}(s).$$

Now $Q_{I,v,q}^{(v_1\alpha_{2r-1}, v_1\alpha_{2r+1})}$ is precisely the set

$$\{\beta \in I : \beta \equiv v \pmod{q},\ \beta = Xv_1\alpha_{2r-1} + Yv_1\alpha_{2r+1} \text{ with } (X,Y) \in \mathbb{Q}^2,\ X > 0,\ Y \ge 0\},$$

and since $(I, q) = 1$, we can replace here v by

$$w = (C_{2r})_q v_1\alpha_{2r-1} + (D_{2r})_q v_1\alpha_{2r}.$$

We now apply Corollary 4.2 with $e = v_1\alpha_{2r-1},\ f = v_1\alpha_{2r},\ e^* = v_1\alpha_{2r+1},\ t = a_{2r+1},\ C = (C_{2r})_q = qc_{2r},\ D = (D_{2r})_q = qc_{2r-1}$, so that $\delta = c_{2r+1}$ and $A = (a_{2r+1}c_{2r} - c_{2r-1} + c_{2r+1})$ by (2.3) and (2.4). Therefore $\zeta_{I,v,q}(0)$ equals

$$\sum_{r=0}^{lm-1}\left((a_{2r+1}c_{2r} - c_{2r-1} + c_{2r+1})(1 - c_{2r}) + \frac{a_{2r+1}}{2}\left(c_{2r}^2 - c_{2r} - \frac{1}{6}\right) + \frac{d_{2r} - d_{2r+2}}{2}\right)$$
$$+ \sum_{r=0}^{lm-1}\left(\mathrm{Tr}\left(\frac{\alpha_{2r}}{4\alpha_{2r-1}}\right)B_2(c_{2r-1}) + \mathrm{Tr}\left(\frac{-\alpha_{2r}}{4\alpha_{2r+1}}\right)B_2(c_{2r+1})\right).$$

Now,

$$-\frac{\alpha_{2r}}{4\alpha_{2r+1}} = \frac{a_{2r+2}}{4} - \frac{\alpha_{2(r+1)}}{4\alpha_{2(r+1)-1}},$$

and so, since $a_{j+L} = a_j,\ c_{j+Lm} = c_j,\ d_{j+Lm} = d_j$ we deduce that

$$\zeta_{I,v,q}(0) = \sum_{j=0}^{Lm-1} (-1)^j \left(\frac{a_j}{2} B_2(d_j) + c_j d_j\right)$$

6. Two-dimensional "Gauss sums"

Throughout this section, we assume $(q, 2d) = 1$.

Let χ be a character $\pmod q$, with $q > 1$, and $h(t) \in \mathbb{Z}[t]$. Define

$$g(\chi, h) := \sum_{0\le n\le q-1} \chi(n)h(n/q).$$

It is well-known that $L(0, \chi) = -g(\chi, t)$. Furthermore, if $\chi(-1) = -1$ then $g(\chi, t^2) = g(\chi, t)$ since

$$g(\chi, t^2) = \sum_{1\le n\le q-1} \chi(n)(n/q)^2 = \sum_{1\le n\le q-1} \chi(q-n)(1-n/q)^2 = -g(\chi, 1)+2g(\chi, t)-g(\chi, t^2).$$

For $f(x, y) = ax^2 + bxy + cy^2$ with $(q, 2d) = 1$ where $d = b^2 - 4ac$, we define

$$g(\chi, f, h) := \sum_{0\le m,n\le q-1} \chi(f(m, n))h(n/q).$$

For ℓ odd we have $\chi(f(m, n))B_\ell(n/q) = -\chi(f(q-m, q-n))B_\ell((q-n)/q)$ by the property of Bernoulli polynomials mentioned below formula (3), and so $g(\chi, f, B_\ell) = B_\ell(0) \sum_{0\le m\le q-1} \chi(f(m, 0))$ $B_\ell\chi(a) \sum_{0\le m\le q-1} \chi^2(m)$ which equals 0 unless $\ell = 1$ and χ has order dividing 2 in which case we get $-\chi(a)\phi(q)/2$.

For $h = 1$ ($\ell = 0$ above) we note that there exists $g \pmod q$ such that $\chi(g) \ne 0, 1$, and that one can show there exist integers r, s for which $r^2 - ds^2 \equiv g \pmod q$. But then replacing the integers m, n by M, N in the sum where $(aM + bN) + \sqrt{d}N = ((am + bn) + \sqrt{d}m)(r + \sqrt{d}s)$ we find that the sum equals itself times $\chi(g)$ and thus $g(\chi, f, 1) = 0$.

Factoring $q = \prod_i p_i^{e_i}$ we can write $\chi = \prod_i \chi_i$ where χ_i is a primitive character mod $p_i^{e_i}$ for each i. Then χ_- is the product of the χ_i of order two (and thus $\chi_-(.) = (./q_-)$), and χ_+ is the product of the χ_i of order ≥ 3.

By the Chinese Remainder Theorem, for any polynomial $F(x, y) \in \mathbb{Z}[x, y]$, we have

$$\sum_{m=0}^{q-1} \chi(F(m, n)) = \prod_i \sum_{m_i=0}^{p_i^{e_i}-1} \chi_i(F(m_i, n)). \tag{6.1}$$

If $\chi \pmod p$ has order > 2 then $|J_\chi| = \sqrt{p}$; if χ has order 2 then $J_\chi = -\left(\frac{-1}{p}\right)$. Moreover one has that $J_\chi = \prod_i J_{\chi_i}$.

Proposition 6.1. *Let χ be a primitive character mod $q > 1$, and ℓ an even positive integer. Let $c_\ell := B_\ell/\zeta(\ell) = 2(-1)^{\ell/2+1} l!/(2\pi)^\ell$. Then*

$$g(\chi, f, B_\ell) = c_\ell \overline{\chi}(a)\chi(d)\left(\frac{d}{q}\right)\chi(-1)\tau(\chi)^2 L(\ell, \overline{\chi}^2)$$

Note that this also holds if $\chi = 1$ in which case $L(\ell, \overline{\chi}^2) = \zeta(\ell)$, so that the above reads $B_l = c_\ell \zeta(\ell)$.

The expression on the right hand side here involves an infinite product. However we can rewrite this as

$$g(\chi, f, B_\ell) = \overline{\chi}(a)\chi(d)\left(\frac{d}{q}\right)\beta_{\chi,\ell}$$

where

$$\beta_{\chi,\ell} := \chi_+(-1)J_{\chi+}g(\chi^2, B_\ell)\mu(q_-)\prod_{p|q_-}\left(\frac{p^\ell\chi_+^2(p)-1}{p^{\ell-1}\chi_+^2(p)-1}\right),$$

something that can evidently be determined in a finite number of steps. Note that if χ has order 2 then $\beta_{\chi,\ell} = qB_\ell\mu^2(q)\prod_{p|q}(1-p^{-\ell})$. We also have $\beta_{\chi,2} = \beta_\chi$.

Lemma 6.2. *Let ψ be a character* (mod Q) *which induces χ* (mod q). *Then*

$$g(\chi, B_\ell) = \frac{g(\psi, B_\ell)}{(q/Q)^{\ell-1}}\prod_{p|q, p\nmid Q}(1-p^{\ell-1}\psi(p)).$$

Proof. By writing $N = n + jQ$ we find, by (4.1), that

$$\sum_{N=0}^{kQ-1}\psi(N)B_\ell(N/kQ) = \sum_{n=0}^{Q-1}\psi(n)\sum_{j=0}^{k-1}B_\ell(n/kQ + j/k) = k^{-(\ell-1)}g(\psi, B_\ell). \tag{6.3}$$

Let $m = \prod_{p|q, p\nmid Q} p$. Then, writing $n = Nd$, we have that $g(\chi, B_\ell)$ equals

$$\sum_{\substack{n=0\\(n,m)=1}}^{q-1}\psi(n)B_\ell(n/q) = \sum_{d|m}\mu(d)\sum_{N=0}^{q/d-1}\psi(dN)B_\ell(N/(q/d)) = \sum_{d|m}\mu(d)\psi(d)\frac{g(\psi, B_\ell)}{(q/dQ)^{\ell-1}},$$

by (6.3), and the result follows.

Lemma 6.3. *Let χ be a primitive character* (mod q), *where q is power of prime p. Then*

$$\sum_{r=0}^{q-1}\chi(dr^2 - p^f) = \left(\frac{d}{q}\right)\cdot\begin{cases}\chi(-4)J_\chi & \text{if } f = 0\\ (p-1) & \text{if } f \geq 1 \text{ and } \chi(.) = (./p)\\ 0 & \text{if } f \geq 1 \text{ otherwise.}\end{cases}$$

Proof. If $q \geq p^2$ and $f \geq 1$ then we see that if $p \nmid r_0$ then $\{dr^2 - p^f : 0 \leq r \leq q-1,\ r \equiv r_0 \pmod p\} = \{(dr_0^2 - p^f)(1+ps) : 0 \leq s \leq q/p - 1\}$ and so we see that the sum over these r is 0.

If $q = p$ and $f \geq 1$ then our sum is $\chi(d) \sum_{0 \leq r \leq p-1} \chi^2(r)$.

If $f = 0$ write $q = p^e$ where $e = 2k \geq 2$ or $2k - 1 \geq 3$ for some $k \geq 1$. The terms for which $p^k | r$ contribute $\chi(-1)p^{e-k}$ to the sum, in total. The other terms are partitioned according to the power of p dividing r. So, writing $r = p^j R$ with $p \nmid R$, we obtain the sum

$$\sum_{j=0}^{k-1} \sum_{\substack{R=1 \\ p \nmid R}}^{p^{e-j}} \chi(dp^{2j}R^2 - 1). \tag{6.4}$$

Note that for $j \leq k-1$, $\{dp^{2j}R^2 - 1 :\ 1 \leq R \leq p^{e-j}, R \equiv R_0 \pmod p\} = \{(dp^{2j}R_0^2 - 1)(1 + p^{2j+1}s) :\ 1 \leq s \leq p^{e-j-1}\}$ if $p \nmid R_0(dp^{2j}R_0^2 - 1)$, and thus this subsum equals 0 unless $j = k-1$ and $e = 2k-1$. Thus if $e = 2k$ is even, the sum in (6.4) is 0 and our total is $\chi(-1)p^k$. If $e = 2k - 1 \geq 1$ is odd our total is

$$\chi(-1)p^{k-1} + \sum_{\substack{R=1 \\ p \nmid R}}^{p^k} \chi(dR^2 q/p - 1) = p^{k-1}\chi(-1) \sum_{j=0}^{p-1} \left(1 + \left(\frac{dj}{p}\right)\right) \chi(1 - jq/p),$$

which equals $p^{k-1}\chi(-1) \left(\frac{d}{p}\right) \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \chi(1 - jq/p)$. Notice that this is (d/p) times the same sum with $d = 1$. However if $d = 1$ we see, by taking $r = 1 + 2m$, that our sum equals $\chi(-4)J_\chi$, and thus the result.

If $q = p$ and $f = 0$ note that if $(\nu/p) = -1$ then the union of the two sets $\{\nu r^2 - 1 : 0 \leq r \leq p-1\}$ and $\{r^2 - 1 : 0 \leq r \leq p-1\}$ gives us two copies of $\{r : 0 \leq r \leq p-1\}$, and so our sum equals (d/p) times the sum with $d = 1$. But then writing $r = 2m + 1$ we obtain $\chi(-4)(d/p)J_\chi$.

Corollary 6.4. *Let χ be a primitive character $\pmod q$. Then*

$$\sum_{m=0}^{q-1} \chi(m^2 - dn^2) = \chi_+(-4dn^2) \left(\frac{d}{q_+}\right) J_{\chi_+} \mu(q_-/(n, q_-))\phi((n, q_-)).$$

Proof. By (6.1) we have

$$\sum_{m=0}^{q-1} \chi(m^2 - dn^2) = \prod_i \sum_{m_i=0}^{p_i^{e_i}-1} \chi_i(m_i^2 - dn^2).$$

By Lemma 6.3 the ith term is zero if $p_i | (n, q_+)$, and thus the whole product. Therefore we now assume that $(n, q_+) = 1$. If $p_i | q_+$ then, by replacing m_i by dnr, our sum becomes $\chi_i(dn^2) \sum_{r=0}^{p_i^{e_i}-1} \chi_i(dr^2 - 1)$; and so the total contribution of q_+ is, by Lemma 6.3,

$$\chi_+(-4dn^2) \left(\frac{d}{q_+}\right) J_{\chi_+}.$$

Let $g=(n,q_-)$. If $p|(q_-/g)$ then, similarly we have

$$\sum_{m=0}^{p-1}\left(\frac{m^2-dn^2}{p}\right)=\left(\frac{d}{p}\right)\sum_{r=0}^{p-1}\left(\frac{dr^2-1}{p}\right)=\left(\frac{d}{p}\right)^2\left(\frac{-1}{p}\right)^2(-1)=-1$$

since $J_{(./p)}=-(-1/p)$; and if $p|g$ then our sum is simply $p-1$. Therefore the total contribution of q_- is $\mu(q_-/g)\phi(g)$.

Proof of Proposition 6.1. For now assume, that $(a,q)>1$. If $p|(a,q)$ then the result will follow from (6.1), and from the result for $q=p^e$, which we now prove: Since $p|a$ we know that $p\not|b$ (as $p\not|d$). We may assume $p\not|n$ else the sum is 0. But then $p\not|2am+bn$, and so, by Hensel's lemma, for each $m_0 \pmod p$ with $p\not|f(m_0,n)$ we have $\{f(m,n) \pmod q : m\equiv m_0 \pmod p, 0\le m\le q-1\}=\{f(m_0,n)(1+rp) \pmod q : 0\le r\le q/p-1\}$; and thus the sum over such m is 0, unless $q=p$. In that case we write $\chi(f(m,n))=\chi(r)\chi(n)$ where $r=bm+cn$ varies over the elements $\pmod p$ as m does, and thus our sum is 0.

So now assume that $(a,q)=1$, and therefore $\chi(f(m,n))=\overline{\chi}(4a)\chi(r^2-dn^2)$ where $r=2am+bn$, and so r varies over the elements $\pmod q$ as m does. We now substitute in Corollary 6.4 to obtain that our sum equals $\overline{\chi}(a)\chi(d)\left(\frac{d}{q}\right)\chi_+(-1)J_{\chi_+}$ times

$$\sum_{0\le n\le q-1}\chi_+^2(n)B_\ell(n/q)\mu(q_-/(n,q_-))\phi((n,q_-))=\sum_{g|q_-}\sum_{\substack{0\le n\le q-1\\(n,q_-)=g}}\chi_+^2(n)B_\ell(n/q)\mu(q_-/g)\phi(g)$$

$$=\sum_{g|q_-}\mu(q_-/g)\phi(g)\chi_+^2(g)\sum_{\substack{0\le N\le q/g-1\\(N,q_-/g)=1}}\chi_+^2(N)B_\ell(N/(q/g))$$

writing $n=Ng$. In this last sum we can replace χ_+^2 by $\chi_{++} \pmod{q/g}$, the character induced by χ_+^2, so that the sum equals $g(\chi_{++},B_\ell)$. By Lemma 6.2 this equals $g(\chi_+^2,B_\ell)$ times

$$\sum_{g|q_-}\mu(q_-/g)\phi(g)\chi_+^2(g)\frac{1}{(q_-/g)^{\ell-1}}\prod_{p|(q_-/g)}(1-p^{\ell-1}\chi_+^2(p))$$
$$=\frac{1}{q_-^{\ell-1}}\prod_{p|q_-}\left(p^{\ell-1}(p-1)\chi_+^2(p)-(1-p^{\ell-1}\chi_+^2(p))\right),$$

and thus $g(\chi,f,B_\ell)=\overline{\chi}(a)\chi(d)\left(\frac{d}{q}\right)\beta_{\chi,\ell}$ after another application of Lemma 6.2.

The functional equation yields, for a primitive character $\psi \pmod q$ where $q>1$ and $\psi(-1)=1$ (see, e.g. Chapter 4 of [8]), that $L(1-\ell,\psi)=0$ if ℓ is odd, and

$$L(1-\ell,\psi)=2(-1)^{\ell/2}\Gamma(\ell)\left(\frac{q}{2\pi}\right)^\ell\frac{\tau(\psi)}{q}L(\ell,\overline{\psi})$$

if ℓ is even. Now, in (4), we saw that $L(1-\ell,\psi) = -q^{\ell-1}g(\psi,B_\ell)/\ell$, and so, if ℓ is even then

$$g(\psi,B_\ell) = c_\ell \tau(\psi) L(\ell,\overline{\psi}). \tag{6.5}$$

Now, in the proof above we have that χ_+^2 is primitive $\pmod{q_+}$ and that

$$\beta_{\chi,\ell} = \chi_+(-1) J_{\chi_+} \frac{1}{q_-^{\ell-1}} \prod_{p|q_-} (p^\ell \chi_+^2(p) - 1) g(\chi_+^2, B_\ell),$$

which, when combined with (6.5) taking $\psi = \chi_+^2$, equals

$$c_\ell \chi_+(-1) J_{\chi_+} \tau(\chi_+^2) q_- \chi_+^2(q_-) L(\ell, \overline{\chi}^2)$$

since $\prod_{p|q_-}(p^\ell\chi_+^2(p)-1)L(\ell,\overline{\chi_+^2}) = q_-^\ell \chi_+^2(q_-)L(\ell,\overline{\chi}^2)$.

Suppose that ψ_j is a character mod q_j for $j = 1,2$ where $(q_1,q_2) = 1$. Writing each $c \pmod{q_1q_2}$ as $bq_1 + aq_2 \pmod{q_1q_2}$ we obtain, from definition, that $\tau(\psi_1\psi_2) = \sum_{c \pmod{q_1q_2}} (\psi_1\psi_2)(c) e^{2i\pi c/q_1q_2} = \sum_{a \pmod{q_1}} \sum_{b \pmod{q_2}} \psi_1(aq_2)\psi_2(bq_1) e^{2i\pi a/q_1} e^{2i\pi b/q_2} = \psi_1(q_2)\psi_2(q_1)\tau(\psi_1)\tau(\psi_2)$. We also note that since χ_- has order 2 thus $\tau(\chi_-)^2 = \chi_-(-1)q_-$; and also, since χ_+ is primitive thus $\tau(\chi_+^2)J_{\chi_+} = \tau(\chi_+)^2$ (we present a proof of this identity below. Combining all of this information with $\psi_1 = \chi_+^2$, $\psi_2 = \chi_-$ yields

$$\begin{aligned}\chi(-1)\tau(\chi)^2 &= \chi_+(-1)\chi_-(-1)(\chi_+(q_-)\chi_-(q_+)\tau(\chi_+)\tau(\chi_-))^2 \\ &= \chi_+(-1)\chi_-(-1)\chi_+^2(q_-)\tau(\chi_+^2)J_{\chi_+}\chi_-(-1)q_- = \chi_+(-1)J_{\chi_+}\tau(\chi_+^2)q_-\chi_+^2(q_-).\end{aligned}$$

We therefore deduce the result.

We end this section by proving the identity $\tau(\chi_+^2)J_{\chi_+} = \tau(\chi_+)^2$ used above.

Note that if $\chi_j \pmod{q_j}$ are primitive characters with $(q_1,q_2) = 1$ then $J_{\chi_1\chi_2} = J_{\chi_1}J_{\chi_2}$ is immediate from definition.

Now, by the definition of χ_+, we can write $\chi_+ = \chi_1\chi_2\dots\chi_k$ where $\chi_j \pmod{q_j}$ are primitive of order > 2 and the q_j are powers of distinct primes. We will prove our identity for each prime power and then we can deduce the result since

$$\tau((\chi_1\chi_2)^2)J_{\chi_1\chi_2} = \chi_1^2(q_2)\chi_2^2(q_1)\tau(\chi_1^2)\tau(\chi_2^2)J_{\chi_1}J_{\chi_2} = (\chi_1(q_2)\chi_2(q_1)\tau(\chi_1)\tau(\chi_2))^2 = \tau(\chi_1\chi_2)^2.$$

So suppose χ is a primitive character of order > 2, modulo q, a power of prime $p > 2$. The sums below are over all of the residues mod q. Fix pm where $1 \le m \le q/p$. We will show that if $q > p$ then $\sum_{a+b\equiv pm \pmod{q},\ a\equiv a_0 \pmod{q/p}} \chi(a)\chi(b) = 0$ for any a_0, so that $\sum_{a+b\equiv pm \pmod{q}} \chi(a)\chi(b) = 0$: If $p|a_0$ then each $\chi(a) = 0$ and we are done. Otherwise, writing $a = a_0 + k(q/p) = a_0(1 + k(q/p)/a_0)$ so that $b \equiv pm - a_0 - k(q/p) = (pm-a_0)(1+k(q/p)/a_0) \pmod{q}$, our sum becomes $\chi(a_0)\chi(pm-a_0)$ times $\sum_{1\le k\le p}\chi(1+k(q/p)/a_0)^2 = \sum_{1\le k\le p}\chi(1+2(q/p)/a_0)^k = 0$, since χ has order > 2 and $p \ne 2$. Now if

$q = p$ then $\sum_{a+b\equiv 0 \pmod p} \chi(a)\chi(b) = \chi(-1)\sum_a \chi^2(a) = 0$ since χ has order > 2. Thus we have proved $\sum_{a+b\equiv n \pmod q} \chi(a)\chi(b) = 0$ whenever $p|n$.

For $(n,p) = 1$, by writing $a \equiv nA, b \equiv nB \pmod q$, we obtain $\sum_{a+b\equiv n \pmod q} \chi(a)\chi(b) = \chi^2(n)\sum_{A+B\equiv 1 \pmod q} \chi(A)\chi(B) = \chi^2(n)J_\chi$. Thus we have

$$\tau(\chi^2)J_\chi = \sum_{(n,p)=1} \chi^2(n)J_\chi e(n/q) = \sum_n \sum_{a+b\equiv n \pmod q} \chi(a)\chi(b)e(n/q) = \tau(\chi)^2.$$

7. Simplifying the formulae

Let χ be a character of conductor q. One knows that if $\chi(-1) = 1$ then $\zeta_I(0,\chi) = 0$ so we will assume henceforth that $\chi(-1) = -1$. We assume that $(q,d) = 1$.

Let $L = [2,\ell]$ denote the least even period of the expansion, and $l = L/2$.

Let

$$\zeta_I^+(s,\chi) = \zeta_{Cl(I)}^+(s,\chi) := \sum_a \frac{\chi(Na)}{(Na)^s},$$

where the sum is over all integral ideals of K which are equivalent to I in the sense that $a = (\beta)I$ with $\beta \gg 0$.

We first evaluate this function at 0 in the following theorem, and then we deduce Theorem 1.

Theorem 1*. *Suppose that χ is a primitive character mod $q > 1$ where $(q,2d) = 1$ and $\chi(-1) = -1$. We have*

$$\zeta_I(0,\chi)/(L/\ell) = \sum_{j=1}^{\ell} G(f_j,\chi) + \frac{1}{2}\chi(d)\left(\frac{d}{q}\right)\beta_\chi \sum_{j=1}^{\ell} a_j\overline{\chi}(f_j(1,0)).$$

Note that $P_{I,v,q} = P_{I,\epsilon_+ v,q}$, since we may replace β by $\beta\epsilon_+$ in the definition of the set P. As noted at the end of section 2 we have $C_{j+L}(v\epsilon_+) = C_j(v)$ and $D_{j+L}(v\epsilon_+) = D_j(v)$. Inserting these observations into Theorem 3.1 gives that $\zeta_{I,v,q}(0) = \sum_{w\in V} Z_{I,w,q}$ where $V = \{v\epsilon_+^i :\ 0 \le i \le m-1\}$ and

$$Z_{I,w,q} := \sum_{j=1}^{L} (-1)^j \left(c_j(w)d_j(w) + \frac{1}{2}\ a_j B_2(d_j(w)) \right). \tag{7.1}$$

Note that $\zeta_{Cl(I)}^+(s,\chi) = \zeta_{Cl(I^{-1})}^+(s,\chi)$ by definition. Moreover $\zeta_{Cl(I^{-1})}^+(s,\chi) = (NI^{-1})^{-s}\sum_{b\in P_I} \chi(Nb/NI)(Nb)^{-s}$ where $P_I = \{b \in P_F(K) :\ b = (\beta)$ for some $\beta \in I, \beta \gg 0\}$ by definition, so that $\zeta_I^+(0,\chi) = \sum_{v\in R} \chi((v\overline{v})/NI)\zeta_{I,v,q}(0)$. Here R is a complete system of representatives of the equivalence classes of the set $\{v \in I : (v,q) = 1\}$ by the following equivalence relation: v is equivalent to v^* if and only if $v^* \equiv v\epsilon_+^j \pmod q$ for some $j \in \mathbb{Z}$. Inserting (7.1) we obtain, for the set $W := \{w \pmod q :\ w \in I \text{ and } (w,q)=1\}$,

$$\zeta_I^+(0,\chi) = \sum_{v\in R} \chi\left(\frac{v\overline{v}}{NI}\right) \zeta_{I,v,q}(0) = \sum_{w\in W} \chi\left(\frac{w\overline{w}}{NI}\right) Z_{I,w,q}$$
$$= \sum_{j=1}^{L} (-1)^j \sum_{w\in W} \chi\left(\frac{w\overline{w}}{NI}\right) \left(c_j(w)d_j(w) + \frac{1}{2}\, a_j B_2(d_j(w))\right).$$

In fact $W = \{\nu \pmod q : (\nu,q)=1\}$. To see this note that W contains an element from every congruence class modulo q which is coprime to q, since if ν is any algebraic integer of the field which is prime to q, then $\nu NI^{\phi(q)}$ is in I, and it is congruent to ν modulo q (remember that $(q,I)=1$). Therefore

$$\zeta_I^+(0,\chi) = \sum_{j=1}^{L} (-1)^j \sum_{0\le C,D\le q-1} \chi(Q_j(C,D)) \left(\frac{C}{q}\cdot\frac{D}{q} + \frac{a_j}{2} B_2\left(\frac{D}{q}\right)\right)$$
$$= \sum_{j=1}^{L} (-1)^j \left(G(Q_j,\chi) + \frac{a_j}{2}\, g(\chi,Q_j,B_2)\right).$$

Note that if ℓ is odd then $l=\ell$ and $Q_{j+l} = -Q_j$ for all $j\ge 0$, as well as $a_{j+l}=a_j$, so that $G(Q_{j+l},\chi) = -G(Q_j,\chi)$. Note also that $f_j = (-1)^j Q_j$; and that $g(\chi,f_j,B_2(t)) = \overline{\chi}(f_j(1,0))\chi(d)\left(\frac{d}{q}\right)\beta_{\chi,2}$ by Proposition 6.1. Therefore the above can be rewritten as

$$\zeta_I^+(0,\chi)/(L/\ell) = \sum_{j=1}^{\ell} G(f_j,\chi) + \frac{1}{2}\chi(d)\left(\frac{d}{q}\right)\beta_{\chi,2}\sum_{j=1}^{\ell} a_j\overline{\chi}(f_j(1,0)),$$

which is Theorem 1*.

Now, we can compute very easily $\zeta_I(0,\chi)$, using Theorem 1*. Indeed, if ℓ is odd, then there is a unit of norm -1 in K, so $\zeta_I(s,\chi) = \zeta_I^+(s,\chi)$. Hence we may assume that ℓ is even. Then

$$\zeta_I(s,\chi) = \zeta_I^+(s,\chi) + \zeta_{(\alpha)I}^+(s,\chi),$$

since $\alpha>0$ and $\overline{\alpha}<0$. We prove that $\zeta_I^+(0,\chi) = \zeta_{(\alpha)I}^+(0,\chi)$, and then we will know that

$$\zeta_I(0,\chi)/2 = \zeta_I^+(0,\chi)/(L/\ell)$$

in every case.

So we prove that $\zeta_I^+(0,\chi) = \zeta_{(\alpha)I}^+(0,\chi)$, if ℓ is even. A basis of $(\alpha)I$ with the required properties is

$$(v_1^*, v_2^*) := (v_2\alpha, (v_1 - a_1 v_2)\alpha).$$

Indeed, it is easy to see that $(v_2, v_1 - a_1 v_2)$ is a basis of I, $v_2\alpha = v_1\alpha^2 \gg 0$, and

$$\alpha^* := \frac{v_2^*}{v_1^*} = \frac{1}{\alpha} - a_1 = [0, \overline{a_2, a_3 \dots, a_\ell, a_{\ell+1}}] =: [0, \overline{a_1^*, \dots, a_\ell^*}].$$

Define the numbers α_n^* for $n \geq -1$ analogously with respect to α^*, as α_n are defined with respect to α, and let

$$f_j^*(x,y) = (-1)^j (v_1^*\alpha_{j-1}^* x + v_1^*\alpha_j^* y)(\overline{v_1^*\alpha^*}_{j-1} x + \overline{v_1^*\alpha^*}_j y)/N((\alpha)I) \qquad \text{for } j = 1, 2, \dots$$

Then $\alpha_{-1}^* = 1$ and $\alpha_0^* = -\alpha^* = a_1 - \frac{1}{\alpha}$, so we can easily prove (using the recursion formulas and $a_j^* = a_{j+1}$) that

$$\alpha_j^* = \frac{\alpha_{j+1}}{-\alpha}$$

for every $j \geq -1$. This implies also $f_j^* = f_{j+1}$, so, using Theorem 1^*, we are done, i.e. Theorem 1 is proved..

8. Further special values: Theorem 2

Shintani in [5], Theorem 1 showed that $\zeta(1-k, A, (x.y))$ equals $(k-1)!^2$ times the coefficient of $U^{2(k-1)}Z^{k-1}$ in (we write $x^* = 1-x$ and $y^* = 1-y$)

$$(8.1) \qquad \frac{1}{2}\left\{ \frac{e^{U(Z(ax^*+by^*)+(cx^*+dy^*))}}{(e^{U(aZ+c)}-1)(e^{U(bZ+d)}-1)} + \frac{e^{U((ax^*+by^*)+Z(cx^*+dy^*))}}{(e^{U(a+cZ)}-1)(e^{U(b+dZ)}-1)} \right\},$$

which is a polynomial in x^* and y^*. It is convenient to make a change of variables, replacing UZ by z, and U by u, so that the first of these two terms equals

$$(8.2) \qquad \frac{e^{(az+cu)x^*}}{e^{az+cu}-1} \cdot \frac{e^{(bz+du)y^*}}{e^{bz+du}-1}$$

and the second is the same but with u and z interchanged. We may expand this using (3), and it is then tempting to state that we seek the coefficient of $(uz)^{k-1}$; however this is only really valid for polynomial terms, for some care must be taken with the "expansion" of $1/(az+cu)$, since we do not know, with this choice of variables, whether to expand around $z = 0$ or $u = 0$. Tracing this back to the variables U and Z, we see that we should in fact expand around $z = 0$. As we mentioned above, if we interchange u and z then the two functions in (8.1) appear to be identical, but in fact we must expand around $u = 0$ in the second term. Thus we can combine the two expressions so long as, for the non-polynomial terms, we take the mean value of the two polynomials that appear from the two possible expansions (and this is the meaning we use henceforth). Therefore, using $B_n(1-x) = (-1)^n B_n(x)$, we see that $\zeta(1-k, A, (x,y))$ equals $(k-1)!^2$ times

$$(8.3) \qquad \sum_{\substack{r,s\geq 0\\ r+s=2k}} \frac{B_r(x)}{r!}\frac{B_s(y)}{s!} \sum_{\substack{h,i\in\mathbb{Z}\\ h+i=k-1}} \binom{r-1}{h}\binom{s-1}{i} a^h b^i c^{r-1-h} d^{s-1-i}.$$

We now develop the generalization of Corollary 4.2, taking our matrix to be as in Corollary 4.2, and now writing $e = \alpha$, $e^* = \beta = e + t\gamma$, $f = \gamma$. (that is, we take $a = \alpha$, $b = \beta$, $c = \overline{\alpha}$, $d = \overline{\beta}$ above). We wish to sum over the values (x_j, y_j) where $y_j = (d+j)/t$ for $0 \le j \le t-1$, while $x_j = c - y_j$ if $0 \le j < A$, and $x_j = c + 1 - y_j$ if $A \le j < t$. Now if $x = C - y$ then the exponent in the numerator of (8.2) is $CL + tNy$ where, for convenience, we temporarily write

$$L = z\alpha + u\overline{\alpha},\ M = z\beta + u\overline{\beta},\ N = z\gamma + u\overline{\gamma}, \tag{8.4a}$$

with $M = L + tN$. Thus the sum of the numerators in our range is

$$\begin{aligned} e^{cL+Nd}\left((1-e^L)\sum_{j=0}^{A-1} e^{Nj} + e^L \sum_{j=0}^{t-1} e^{Nj}\right) &= \frac{e^{cL+Nd}}{1-e^N}\left((1-e^L)(1-e^{NA}) + e^L(1-e^{Nt})\right), \\ &= \frac{e^{cM+\delta N}(e^L-1) - e^{cL+dN}(e^M-1)}{1-e^N}, \end{aligned}$$

where $\delta = d + A - tc$. Therefore $Z(1-k)$ is $(k-1)!^2 q^{2(k-1)}$ times the coefficient of $(uz)^{k-1}$ in

$$\frac{e^{cL}}{e^L-1} \cdot \frac{e^{dN}}{e^N-1} \ - \ \frac{e^{cM}}{e^M-1} \cdot \frac{e^{\delta N}}{e^N-1}. \tag{8.4b}$$

Next we make the substitutions of section 5 (writing $\beta_j = v_1 \alpha_j$ for convenience). When we take the sum over r (as there) we obtain that

$$\zeta_{I,v,q}(1-k) = (k-1)!^2 q^{2(k-1)} \sum_{j=0}^{Lm-1} (-1)^j T_j(v)$$

where, using the same expansion as in (8.3),

$$\begin{aligned} T_j(v) :&= \text{coeff of } (uz)^{k-1} \text{ in } \ \frac{e^{c_j(z\beta_{j-1}+u\overline{\beta}_{j-1})}}{e^{z\beta_{j-1}+u\overline{\beta}_{j-1}}-1} \cdot \frac{e^{c_{j-1}(z\beta_j+u\overline{\beta}_j)}}{e^{z\beta_j+u\overline{\beta}_j}-1} \\ &= \sum_{\substack{r,s\ge 0\\ r+s=2k}} B_r(c_j)B_s(d_j)p_{r,s}(\beta_{j-1},\beta_j) \end{aligned}$$

since $c_{j-1} = d_j$. Noting that $p_{r,s}(\eta x, \eta y) = (N\eta)^{k-1} p_{r,s}(x,y)$ for any $0 \ll \eta \in K$, by definition, we see that each $p_{r,s}(\beta_{j-1},\beta_j) = (Nv_1)^{k-1} p_{r,s}(\alpha_{j-1},\alpha_j)$. Moreover since $\alpha_{j+L} = \epsilon_+\alpha_j$, $c_{j+L}(v\epsilon_+) = c_j(v)$ and $d_{j+L}(v\epsilon_+) = d_j(v)$, we thus deduce that $T_{j+L}(v\epsilon_+) = T_j(v)$. Hence we can obtain the analogy to (7.1), and from these we deduce Theorem 2, as in section 7.

Remark. When we specialize Theorem 2 to the case $k = 1$ (that is, Theorem 1), we obtain

$$\zeta_I(0,\chi) = 2\sum_{j=1}^{\ell} \sum_{0\le m,n\le q-1} \chi(f_j(m,n))\times$$

$$\left\{\frac{1}{4}\left(\frac{\overline{\alpha_j}}{\overline{\alpha_{j-1}}}+\frac{\alpha_j}{\alpha_{j-1}}\right)B_2\left(\frac{n}{q}\right)+B_1\left(\frac{m}{q}\right)B_1\left(\frac{n}{q}\right)+\frac{1}{4}\left(\frac{\overline{\alpha_{j-1}}}{\overline{\alpha_j}}+\frac{\alpha_{j-1}}{\alpha_j}\right)B_2\left(\frac{m}{q}\right)\right\}$$

and there is no obvious cancellation here. However if we look at the $T_j(v)$, then the two outer terms here correspond there to

$$\frac{1}{4}\sum_{j=0}^{Lm-1}(-1)^j\left\{\left(\frac{\overline{\alpha_j}}{\overline{\alpha_{j-1}}}+\frac{\alpha_j}{\alpha_{j-1}}\right)B_2\left(c_{j-1}\right)+\left(\frac{\overline{\alpha_{j-1}}}{\overline{\alpha_j}}+\frac{\alpha_{j-1}}{\alpha_j}\right)B_2\left(c_j\right)\right\}$$

which surprisingly equals $\frac{1}{2}\sum_{j=0}^{Lm-1}(-1)^j a_j B_2(c_{j-1})$, since $\alpha_j/\alpha_{j-1} = a_j + \alpha_{j-2}/\alpha_{j-1}$. Carrying this simplification back through the argument gives us that

$$\zeta_I(0,\chi) = 2\sum_{j=1}^{\ell} \sum_{0\le m,n\le q-1} \chi(f_j(m,n))\left\{B_1\left(\frac{m}{q}\right)B_1\left(\frac{n}{q}\right)+\frac{a_j}{2}B_2\left(\frac{n}{q}\right)\right\}$$

as in Theorem 1. We do not know how to generalize this cancellation for larger k.

9. Examples

We start with a definition. If $f(x,y) = ax^2 + bxy - cy^2$ is a quadratic form with integer coefficients, let $\overline{f}(x,y) = cx^2 + bxy - ay^2$. Note that if $\chi(-1) = -1$, then

$$G(f,\chi) = G(\overline{f},\chi) - g(\overline{f},\chi,t),$$

this can be seen from the change of variables $m \to n$ and $n \to q - m$. Then, if χ has order > 2, we have $G(f,\chi) = G(\overline{f},\chi)$, since we saw near the start of section 6 that $g(\overline{f},\chi,t) = 0$ in this case.

In each case here we explore the principal ideal class, and we assume that χ has order > 2.

Yokoi's discriminants: Let $d = p^2 + 4$ where p is an odd integer. Let $\alpha = (\sqrt{d} - p)/2 = [0, \overline{p}]$ so that $\ell = 1$, with $v_1 = 1, v_2 = \alpha$. Then $f_1(x,y) = x^2 + pxy - y^2$ so that

$$\zeta_I(0,\chi)/2 = \sum_{1\le m,n\le q-1} \chi(m^2 + pmn - n^2)\ \frac{m}{q}\frac{n}{q} + \frac{p}{2}\ \chi(d)\left(\frac{d}{q}\right)\beta_\chi.$$

Chowla's discriminants: Let $d = 4p^2 + 1$ and $\alpha = (\sqrt{d} + 1 - 2p)/2 = [0, \overline{1, 1, 2p-1}]$ so that $\ell = 3$, with $v_1 = 1, v_2 = \alpha$. Then $f_1(x,y) = px^2 + xy - py^2$ with $f_2(x,y) = px^2 + (2p-1)xy - y^2$ and $f_3(x,y) = x^2 + (2p-1)xy - py^2 = \overline{f_2}$ so that

$$\zeta_I(0,\chi)/2 = G(f_1,\chi) + 2G(f_2,\chi) + \left(p - \frac{1}{2} + \overline{\chi}(p)\right)\ \chi(d)\left(\frac{d}{q}\right)\beta_\chi.$$

Mollin's discriminants: Let $d = p^2+4p$ where p is an odd integer, and $\alpha = (\sqrt{d}-p)/2 = [0, \overline{1, p}]$ so that $\ell = 2$, with $v_1 = 1, v_2 = \alpha$. Then $f_1(x, y) = px^2+pxy-y^2$ with $f_2(x, y) = \overline{f_1}$ so that

$$\zeta_I(0, \chi)/2 = 2G(f_1, \chi) + \frac{1}{2}(p + \overline{\chi}(p))\ \chi(d) \left(\frac{d}{q}\right) \beta_\chi.$$

Note that if $h(d) = 1$ then p must be prime else if $p = ab$ then the ideal $(a, (\sqrt{d}-p)/2)$ gives rise to the different continued fraction $(\sqrt{d}-p)/2a = [0, \overline{a, b}]$.

10. Class number one

Let $\zeta_K(s, \chi) = \sum_a \chi(Na)/(Na)^s$ where the sum is over all integral ideals of K. Evidently if $h(d) = 1$ then this is identical to $\zeta_I(s, \chi)$, where I is a principal ideal. On the other hand we know that

$$\zeta_K(s, \chi) = L(s, \chi)L(s, \chi\chi_d)$$

where $\chi_d = (./d)$. Moreover for $d \equiv 1 \pmod 4$ and $\chi(-1) = -1$ we can use (1), to deduce that $\zeta_K(0, \chi) = g(\chi, t)g(\chi\chi_d, t)$. Let $m_\chi := qg(\chi, t)$ and note that $g(\chi\chi_d, t)$ is an algebraic integer in $\mathbb{Z}[\chi]$, see p. 88. of [B1]. Let $A_\chi(p) := q\zeta_I(0, \chi)/2$. Now if $h(d) = 1$ we have $q\zeta_I(0, \chi) = m_\chi g(\chi\chi_d, t)$; and so $m_\chi | 2A_\chi(p)$. Let $B_\chi = q\beta_\chi$ and $C_\chi(p) := q\sum_{j=1}^{\ell} G(f_j, \chi)$. Suppose that $\mathcal{P}$ is a prime ideal which divides m_χ and thus $2A_\chi(p)$, and assume that $(\mathcal{P}, 2B_\chi) = 1$.

If $p \equiv p' \pmod q$ then

- For $d = p^2 + 4$, we have $A_\chi(p) = A_\chi(p') + \frac{1}{2}(p - p')\chi(d)\left(\frac{d}{q}\right) B_\chi$, and so

$$p \equiv p' - \overline{\chi}(d)\left(\frac{d}{q}\right) \frac{2A_\chi(p')}{B_\chi} = -\overline{\chi}(d)\left(\frac{d}{q}\right) \frac{2C_\chi(p')}{B_\chi} \pmod{\mathcal{P}}; \tag{10.1}$$

- Similarly for $d = 4p^2 + 1$ we deduce that

$$p \equiv -\overline{\chi}(d)\left(\frac{d}{q}\right) \frac{C_\chi(p')}{B_\chi} - \overline{\chi}(p') + \frac{1}{2} \pmod{\mathcal{P}}$$

- and for $d = p^2 + 4p$ that

$$p \equiv -\overline{\chi}(d)\left(\frac{d}{q}\right) \frac{2C_\chi(p')}{B_\chi} - \overline{\chi}(p') \pmod{\mathcal{P}}$$

Now if q' is the rational prime dividing the norm of $\mathcal{P}$ then this forces a congruence for $p \pmod{q'}$. In other words, we have a strange phenomena that the value of $p \pmod q$ forces the value of $p \pmod{q'}$, and from this we strive for a contradiction.

We work with some of the same characters from section 4 of [B1]: Characters $\chi_1 \pmod{7\cdot 5^2}$ and $\chi_2 \pmod{61}$, are given on primitive roots as

$$\chi_{1,5^2}(2) \equiv 8 \pmod{\mathcal{P}_1},\ \chi_{1,7}(3) \equiv 47 \pmod{\mathcal{P}_1},\ \text{for a certain prime ideal } \mathcal{P}_1|61;$$
$$\chi_{1,5^2}(2) \equiv 380 \pmod{\mathcal{P}_2},\ \chi_{1,7}(3) \equiv 1406 \pmod{\mathcal{P}_2},\ \text{for a certain prime ideal } \mathcal{P}_2|1861;$$
$$\chi_2(2) \equiv -28 \pmod{\mathcal{P}_3},\ \ \text{for a certain prime ideal } \mathcal{P}_3|1861.$$

Now in each case here we have $B_\chi = -J_\chi \sum_{n=0}^{q-1} \chi^2(n)n^2/q$. Using Maple we find that $B_{\chi_1} \equiv 51 \pmod{61}$, $B_{\chi_2} \equiv 121 \pmod{1861}$, $B_{\chi_3} \equiv 945 \pmod{1861}$.

We use these formulae as follows: Suppose that $h(d) = 1$ for a given p where $\left(\frac{d}{5}\right) = \left(\frac{d}{7}\right) = -1$; and suppose that $p \equiv p_0 \pmod{175}$. Using χ_1 we deduce that $p \equiv p_1 \pmod{61}$, and from this, using χ_2 we deduce that $p \equiv p_3 \pmod{1861}$. On the other hand, using χ_1 we deduce, from $p \equiv p_0 \pmod{175}$, that $p \equiv p_2 \pmod{1861}$. Typically $p_2 \not\equiv p_3 \pmod{1861}$ (using Maple).

For $d = p^2+4$ the exceptions are when $p \equiv \pm3, \pm8, \pm13$ or $\pm17 \pmod{175}$. We discover that, in each of these cases, $p \equiv \pm3, \pm8, \pm13$ or $\pm17 \pmod{175 \times 61 \times 1861}$. But the only ones of these cases for which $\left(\frac{d}{61}\right) = \left(\frac{d}{1861}\right) = -1$ are when $p \equiv \pm13 \pmod{175}$. This is as was found in [B2]; the final case was ruled out by using a character $\chi_3 \pmod{61}$ to show that p belongs to a certain residue class $\pmod{41}$ implying that $\left(\frac{d}{41}\right) = 1$.

For $d = 4p^2 + 1$ the exceptions are when $p \equiv \pm2$ or $\pm13 \pmod{175}$. We discover that, in each of these cases, $p \equiv \pm2$ or $\pm13 \pmod{175 \times 61 \times 1861}$. But the only ones of these cases for which $\left(\frac{d}{61}\right) = \left(\frac{d}{1861}\right) = -1$ are when $p \equiv \pm13 \pmod{175}$. This is as was found in [B2]; the final case was ruled out by using a character $\chi_3 \pmod{61}$ to show that p belongs to a certain residue class $\pmod{41}$ implying that $\left(\frac{d}{41}\right) = 1$.

For $d = p^2 + 4p$ the exceptions are when $p \equiv 2, 9, 19, -23, -13$ or $-6 \pmod{175}$. We discover that, in each of these cases, $p \equiv 2, 9, 19, -23, -13$ or $-6 \pmod{175 \times 61 \times 1861}$. But none of these cases satisfy $\left(\frac{d}{61}\right) = \left(\frac{d}{1861}\right) = -1$.

A nice Corollary of the three theorems (Yokoi, Chowla and Mollin) is the following:

Theorem. *Suppose that* $d \geq 25$ *with* $d \equiv 1 \pmod 4$. *Then* $-n^2 + n + (d-1)/4$ *is prime for* $1 < n < (\sqrt{d} - 1)/2$ *if and only if* $d = 29, 37, 53, 77, 101, 173, 197, 293, 437$ *or* 677.

Remark. These are exactly the set of class number one fields in this range, from our three cases!

Proof. If $d \equiv 1 \pmod 8$ then 2 always divides $-n^2 + n + (d-1)/4$ so we must have $(\sqrt{d} - 1)/2 < 2$, that is $d < 25$, or $2 = -2^2 + 2 + (d-1)/4$ that is $d = 17$. Otherwise assume that $d \equiv 5 \pmod 8$. Note then that every $-n^2 + n + (d-1)/4$ is odd. We will also assume that $d > 100$.

We now show that we may assume that d is squarefree. Suppose $p^2 | d$, then p is odd. Evidently p^2 divides our polynomial when $n = (p+1)/2$. This is in our range unless $d = p^2$; but in this case $d \equiv 1 \pmod 8$, contradiction.

Suppose that $2 < q < \sqrt{d} - 1$ is prime with $\left(\frac{d}{q}\right) = 1$ and $d \not\equiv 1 \pmod q$. Since $\left(\frac{d}{q}\right) = 1$ there exists an odd integer $N, 1 \leq N \leq q - 1$ such that $N^2 \equiv d \pmod q$; and $N \not\equiv 1 \pmod q$ since $d \not\equiv 1 \pmod q$. Let $n = (N+1)/2$, so there exists n, $1 < n \leq (q-1)/2 < (\sqrt{d} - 1)/2$ such that $(2n-1)^2 \equiv d \pmod q$, that is q divides $-n^2 + n + (d-1)/4 = (d - (2n-1)^2)/4$. By hypothesis $-n^2 + n + (d-1)/4$ is prime and so must equal q. Therefore $q = -n^2 + n + (d-1)/4 > \sqrt{d} - 1$ as $n < (\sqrt{d} - 1)/2$, a contradiction.

Suppose that $2 < q < (\sqrt{d} - 3)/2$ is prime with $d \equiv 1 \pmod q$. Then q divides $-n^2 + n + (d-1)/4$ with $n = q+1 < (\sqrt{d} - 1)/2$; but then $q = -n^2 + n + (d-1)/4 > \sqrt{d} - 1$, a contradiction.

Suppose that prime $q|d$ with $q < \sqrt{d} - 2$. Then q divides $-n^2 + n + (d-1)/4$ with $n = (q+1)/2 < (\sqrt{d}-1)/2$; but then $q = -n^2 + n + (d-1)/4 > \sqrt{d} - 1$, a contradiction.

For any quadratic field, every ideal class contains an ideal of norm $a < \sqrt{d}/2$; and each prime factor q of a must satisfy $(d/q) \neq -1$. But then, by the previous paragraphs (since each such q is $< \sqrt{d}/2$) the only possible prime factors of a are prime divisors of $(d-1)/4$ which are $> (\sqrt{d}-3)/2$. There can be at most two such prime divisors, perhaps repeated; and so either $d = 1 + 4p$ with p prime, or $d = 1 + 4p^2$ with p prime, or $d = 1 + 4p(p+2k)$ for $k \geq 1$, where $p, p+2k$ are both prime. In this last case $k = 1$ else $d = 1 + 4p(p+2k) > 1 + (\sqrt{d}-3)(\sqrt{d}+5) > d$, a contradiction. Thus, besides the principal form $(1, 1, -(d-1)/4)$, the only other possible reduced forms are $(p, 1, -p)$ when $d = 1 + 4p^2$ with p prime, or $(p, 1, -(p+2))$ when $d = 1 + 4p(p+2)$ and $p, p+2$ are both prime. However, in the first case one easily sees that $(p, 1, -p)$ is in the same cycle as the principal form (see "Chowla's discriminants" above), and in the second case, for the form to be reduced we need $\sqrt{d} - 1 < 2p$ which is untrue. Therefore $h(d) = 1$.

Next write $d = (2m+1)^2 + 4\ell$ when $1 \leq \ell < 2(m+1)$. Taking $n = m$ we find that $q = 2m + \ell$ is prime. Let $r := 2m + 2 - \ell$ so that $rq = d - (1+\ell)^2$; thus if prime $p|r$ then $(d/p) = 0$ or 1:

- If $p|d$ then $2m + 2 - \ell = r \geq p > \sqrt{d} - 2 > 2m - 1$ (by the above) so $\ell = 1$ or 2. If $\ell = 1$ then $p|(r, d) = (2m+1, (2m+1)^2 + 4) = 1$ which is impossible; if $\ell = 2$ then $p|(r, d) = (2m, (2m+1)^2 + 4) = (m, 5)$, so $p = 5 > \sqrt{d} - 2$ which is impossible.
- If $(d/p) = 1$ and $d \not\equiv 1 \pmod{p}$ then $2m + 2 - \ell = r \geq p > \sqrt{d} - 1 > 2m$ by the above, so $\ell = 1$. Thus $p = r = 2m + 1 = q$ and so $d = p^2 + 4$, a "Yokoi discriminant".
- If $d \equiv 1 \pmod{p}$ then $p > m - 1$, by the above. Also $p|(r, d-1) = (2m+2-\ell, (2m+1)^2 + 4\ell - 1) = (2m+2-\ell, \ell(\ell+2))$. Therefore either $p|\ell$ and so $p|m+1$; or $p|\ell+2$ and so $p|m+2$. In the first case we have $p = m+1$ whence $\ell = p$ so that $d = 4p^2 + 1$, a "Chowla discriminant". In the second case $p = m+2$ whence $\ell = m$ so that $d = 4(p-1)^2 - 3$, in which case $(3/d) = 1$, a contradiction.

Finally we may have that $r = 1$ in which case $\ell = 2m + 1$ and $d = \ell^2 + 4\ell$, a "Mollin discriminant".

Thus we have d of the form $p^2 + 4, 4p^2 + 1$ or $p^2 + 4p$ with $h(d) = 1$ and our previous results give the full list of such d.

11. Theorem 2 for the Yokoi discriminants

Let $d = p^2 + 4$ where p is an odd integer, and $\alpha = (\sqrt{d} - p)/2 = [0, \overline{p}]$. Let I be the principal ideal class. We have $\ell = 1, \alpha_0 = -\alpha$ and $\alpha_1 = \alpha^2$. Therefore, for $r + s = 2k$ we have

$$p_{r,s}(\alpha_0, \alpha_1) = \frac{(-1)^{r-1}}{r!} \frac{1}{s!} \sum_{\substack{h,i \in \mathbb{Z} \\ h+i=k-1}} \binom{r-1}{h} \binom{s-1}{i} \alpha^{h+2i} \overline{\alpha}^{r-1-h+2(s-1-i)}$$

$$= \frac{1}{r!} \frac{1}{s!} \sum_{\substack{h,i \in \mathbb{Z} \\ h+i=k-1}} \binom{r-1}{h} \binom{s-1}{i} (-1)^h \alpha^{2i+1-s}$$

since $\alpha\overline{\alpha}=-1$, noting that $2i+1-s=r-2h-1$. The term with $r-1-h$ in place of h, and $s-1-i$ in place of i has summand $(-1)^{r-1-h}\alpha^{2(s-1-i)+1-s}=(-1)^h(-1)^{r-1}(-1/\overline{\alpha})^{s-1-2i}=(-1)^h(\overline{\alpha})^{2i+1-s}$, the conjugate of of term above, and therefore $p_{r,s}(\alpha_0,\alpha_1)\in\mathbb{Q}$. It is not hard to evaluate $p_{r,s}$ as a polynomial in p: We have for $1\le r,s\le k-1$ that

$$p_{r,s}(-\alpha,\alpha^2)=\frac{1}{(k-1)!rs}\sum_{\substack{0\le j\le m-1\\ j\equiv m-1 \pmod 2}}(-1)^{\frac{3r+1-j}{2}}\frac{p^j}{j!\left(\frac{r-1-j}{2}\right)!\left(\frac{s-1-j}{2}\right)!};$$

notice that $p_{r,s}(-\alpha,\alpha^2)=(-1)^{r+k}p_{s,r}(-\alpha,\alpha^2)$. This also holds for $r=2k$ and

$$p_{0,2k}(-\alpha,\alpha^2)=\frac{1}{2(k!)}\sum_{i=1}^{k}\frac{i!p^{2i-1}}{(2i)!(k-i)!}$$

We have $f(x,y)=x^2+pxy-y^2$, so that

$$G_{r,s}(f,\chi):=\sum_{0\le m,n\le q-1}\chi(m^2+pmn-n^2)B_r\left(\frac{m}{q}\right)B_s\left(\frac{n}{q}\right).$$

Writing $M=q-n,\ N=m$ we get that $G_{r,s}(f,\chi)$ equals

$$\begin{aligned}&=\sum_{\substack{0\le m\le q-1\\ 0\le n\le q-1}}\chi(f(m,n))B_r\left(\frac{m}{q}\right)B_s\left(\frac{n}{q}\right)=\sum_{\substack{0\le N\le q-1\\ 1\le M\le q}}\chi(f(N,-M))B_r\left(\frac{N}{q}\right)B_s\left(1-\frac{M}{q}\right)\\ &=\sum_{\substack{0\le N\le q-1\\ 0\le M\le q-1}}\chi(-f(M,N))(-1)^sB_s\left(\frac{M}{q}\right)B_r\left(\frac{N}{q}\right)=\chi(-1)(-1)^sG_{s,r}(f,\chi)\end{aligned}$$

since $B_m(1-t)=(-1)^mB_m(t)$ and $B_m(1)=B_m(0)$ for $m\ge1$.

Therefore Theorem 2 yields, for or any $k\ge1$,

$$\zeta_I(1-k,\chi)=2(k-1)!^2q^{2(k-1)}\sum_{\substack{r,s\in\mathbb{Z}\\ r+s=2k}}p_{r,s}(\alpha_0,\alpha_1)G_{r,s}(f,\chi).$$

Since $\chi(-1)=(-1)^k$, hence $p_{r,s}G_{r,s}=p_{s,r}G_{s,r}$, and so

$$\zeta_I(1-k,\chi)=2(k-1)!^2q^{2(k-1)}\left\{2\sum_{r=0}^{k-1}p_{r,2k-r}(\alpha_0,\alpha_1)G_{r,2k-r}(f,\chi)+p_{k,k}(\alpha_0,\alpha_1)G_{k,k}(f,\chi)\right\}.$$

If $k=1$ then $p_{1,1}=1,p_{0,2}=p/4$ which yields Theorem 1.

If $k=2$ then $p_{2,2}=-p,p_{1,3}=2,p_{0,4}=(6p+p^3)/48$.

References

1. A. Biró, *Yokoi's conjecture*, Acta Arithmetica **106** (2003), 85-104.
2. A. Biró, *Chowla's conjecture*, Acta Arithmetica **107** (2003), 178-194.
3. D. R. Hayes, *Brumer elements over a real quadratic field*, Exposit. Math. **8** (1990), 137-184.
4. R.A. Mollin, *Quadratics*, CRC Press, Boca Raton, FL, 1996.
5. T. Shintani, *On evaluation of zeta functions of totally real algebraic number fields at non-positive integers*, J. Fac. Sci. Univ. Tokyo **23** (1976), 393-417.
6. T. Shintani, *On special values of zeta functions of totally real algebraic number fields*, Proc. ICM (Helsinki) (1978), 591-597.
7. H.M. Stark, *L-functions at $s = 1$. III. Totally real fields and Hilbert's twelfth problem*, Advances in Math **22** (1976), 64-84.
8. L. C. Washington, *Introduction to cyclotomic fields*, Springer, 1982.
9. D. Zagier, *Valeurs des fonctions zêta des corps quadratique réel aux entiers négatifs*, Astérisque **41-42** (1977), 135–151.