VANISHING AND NON-VANISHING THETA VALUES

Henri Cohen and Don Zagier

Abstract. For a primitive Dirichlet character χ of conductor N set $\Theta(\chi) = \sum_{n\in\mathbb{Z}} n^\epsilon \chi(n)\, e^{-\pi n^2/N}$ (where $\epsilon = 0$ for χ even, $\epsilon = 1$ for χ odd), the value of the associated theta series at its point of symmetry under the modular transformation $\tau \to -1/\tau$. These numbers are related by $\Theta(\chi) = W(\chi)\Theta(\bar\chi)$ to the root number of the L-series of χ and hence can be used to calculate the latter quickly if they do not vanish. We describe experiments showing that $\Theta(\chi) \neq 0$ for all χ with $N \le 52100$ (roughly 500 million primitive characters) except for precisely two characters (up to $\chi \to \bar\chi$), of conductors 300 and 600. The proof that $\Theta(\chi)$ vanishes in these two cases uses properties of Ramanujan's modular function of level 5. We also characterize all χ for which $W(\chi)$ is a root of unity and describe some experimental results concerning the algebraic numbers $\Theta(\chi)/\eta(i)^{1+2\epsilon}$ when N is prime.

For Paulo Ribenboim, whose enthusiasm and good humor have lit up the world of number theory.

§1. Introduction

Let χ be an even primitive Dirichlet character of conductor N. To χ one associates the classical Gauss sum and its normalized version, the root number, defined by

$$G(\chi) \;=\; \sum_{n \pmod N} \chi(n)\, \mathbf{e}(n/N)\,, \qquad W(\chi) \;=\; \frac{G(\chi)}{\sqrt{N}}\,. \tag{1}$$

(Here and in the sequel we use the notations $\mathbf{e}(x) = e^{2\pi i x}$ for $x \in \mathbb{C}$, and also $\zeta_N = \mathbf{e}(1/N)$ for the standard Nth root of unity of order $N \in \mathbb{N}$.) The numerical value of $W(\chi)$ is of interest in many contexts, notably in the computation of values of the Dirichlet L-series $L(s,\chi)$ by the approximate functional equation, and it is therefore reasonable to ask whether there is a quicker approach than the obvious $\mathrm{O}(N)$. One idea is to use the functional equation

$$\theta(\chi, -1/\tau) = W(\chi)\,(\tau/i)^{1/2}\;\theta(\overline{\chi},\tau) \qquad (\tau \in \mathfrak{H} = \text{upper half-plane}) \tag{2}$$

of the theta series

$$\theta(\chi,\tau) \;=\; \sum_{n\in\mathbb{Z}} \chi(n)\, q^{n^2/2N} \qquad (q := \mathbf{e}(\tau))$$

associated to χ at its point of symmetry $\tau = i$. This lets us compute $W(\chi)$ as $\Theta(\chi)/\Theta(\overline{\chi})$, where

$$\Theta(\chi) \;:=\; \sum_{n\in\mathbb{Z}} \chi(n)\, e^{-\pi n^2/N}\,. \tag{3}$$

This is much faster for large N (now only $\mathrm{O}(N^{\frac12+\epsilon})$ steps) because of the very rapid convergence of the series, but it breaks down if $\Theta(\chi)$ vanishes.[1] This suggests the following question, apparently first raised by Louboutin [2]:

[1] One could, however, use L'Hôpital's rule in this case to calculate $W(\chi)$ quickly, or else choose $\tau \neq i$ in (2).

Question: *Is $\Theta(\chi)$ always different from zero?*

We observe that the same question can be posed also for odd primitive characters, now with $\Theta(\chi)$ defined as $\sum_n n\,\chi(n)\,e^{-\pi n^2/N}$, the value at $\tau = i$ of the weight 3/2 cusp form $\theta(\chi,\tau) = \sum_n n\,\chi(n)\,q^{n^2/2N}$ associated to χ.

A computer search, initially for even characters of conductor ≤ 2000, showed that $\Theta(\chi)$ was indeed nearly always non-zero, but, amazingly, found *precisely two* characters (up to complex conjugation), one of conductor 300 and one of conductor 600, for which $\Theta(\chi)$ vanished. More precisely, in a first calculation to 38 decimal digits, only two values of $\Theta(\chi)$ were less than about 10^{-5} in absolute value; these two were numerically equal to zero to 38 digits and remained numerically equal to zero when they were recalculated to 10000 decimal digits. A subsequent much larger calculation, which we will report on briefly in §4, produced no further examples.

This raises two new questions:

(i) to prove rigorously that $\Theta(\chi) = 0$ for the two exceptional characters;
(ii) to understand why there are so few examples.

We can say nothing about the latter question, but will give a proof of the vanishing statement and a discussion of some related issues.

Before stating the theorem, we define the two exceptional characters. The group $(\mathbb{Z}/300\mathbb{Z})^\times$ has the structure $C_2 \times C_2 \times C_{20}$ (C_n = cyclic group of order n), with generators 101, 151, and 277, while the group $(\mathbb{Z}/600\mathbb{Z})^\times$ has the structure $C_2 \times C_4 \times C_{20}$ with generators 301, 151, and 577. We define two even characters χ_1 and χ_2, of order 10 and with conductors 300 and 600, respectively, by

$$\chi_1(101) = \chi_1(151) = -1\,,\ \ \chi_1(277) = \mathbf{e}(2/5)\,, \qquad \chi_2(301) = \chi_2(151) = -1\,,\ \ \chi_2(577) = \mathbf{e}(1/5)\,.$$

Theorem 1. *The number $\Theta(\chi)$ vanishes for the two characters χ_1, χ_2 and their complex conjugates, and for no other primitive characters of conductor ≤ 52100.*

(The search limit corresponds to roughly 250 million even and 250 million odd primitive characters.)

Based on this theorem, one can reasonably conjecture that the only examples of the vanishing of central theta values are the four even characters given. A partial result was proved by Louboutin [2], who showed that for p prime, at least $cp/\log(p)$ of the characters χ of conductor p have $\Theta(\chi) \ne 0$.

Apart from the proof of Theorem 1, the paper contains an identity involving Ramanujan's famous modular function of level 5, a very short proof of Watson's quintuple product identity, a complete characterization of χ for which the root number $W(\chi)$ is a root of unity, and some remarks and numerical computations concerning the algebraic numbers $A(\chi) = \Theta(\chi)/\eta(i)$.

§2. Proof of vanishing

We begin by observing that the characters χ_1 and χ_2 can be written more simply as

$$\chi_1(n) \;=\; \Big(\frac{12}{n}\Big)\,\varepsilon(n)\,, \qquad \chi_2(n) \;=\; \Big(\frac{24}{n}\Big)\,\varepsilon(n)^2\,, \tag{4}$$

where ε is the character of order 5 and conductor 25 defined by $\varepsilon(2) = \mathbf{e}(2/5)$. Equivalently, ε is the even character of conductor 25 defined by

$$n \equiv 1 \pmod 5 \;\Rightarrow\; \varepsilon(n) = \zeta_5^{(n-1)/5}\,, \qquad n \equiv 2 \pmod 5 \;\Rightarrow\; \varepsilon(n) = \zeta_5^{3(n-7)/5}\,. \tag{5}$$

The proof that $\Theta(\chi_1)$ and $\Theta(\chi_2)$ vanish is based on the following pair of identities, whose proof

will be given in §3. Denote by $f(\tau)$ Ramanujan's modular function of level 5, defined by

$$f(\tau) \;=\; q^{1/5}\prod_{n=1}^{\infty}(1-q^n)^{(n/5)} \;=\; \cfrac{q^{1/5}}{1+\cfrac{q}{1+\cfrac{q^2}{\ddots}}}\quad,$$

where $q=\mathbf{e}(\tau)$ as usual. Then we have:

Proposition 1. *For all $\tau\in\mathfrak{H}$ and $a\in\mathbb{Z}$, we have*

$$\begin{aligned}\sum_{n\equiv 1 \pmod 5}\Big(\frac{12}{n}\Big)\zeta_5^{a(n-1)/5}\,q^{n^2/120} \;&=\; \zeta_{25}^{2a}\,\eta(5\tau)\,f\Big(\tau+\frac{2a}{5}\Big)^{-1},\\ \sum_{n\equiv 2 \pmod 5}\Big(\frac{12}{n}\Big)\zeta_5^{a(n-7)/5}\,q^{n^2/120} \;&=\; -\zeta_{25}^{-a}\,\eta(5\tau)\,f\Big(\tau+\frac{a}{5}\Big).\end{aligned}\tag{6}$$

Applying these two identities with $a=1$ and $a=-2$, respectively, and adding, we find the formula

$$\begin{aligned}\frac{1}{2}\,\theta(\chi_1,\tau) \;&=\; \sum_{n\equiv 1 \pmod 5}\Big(\frac{12}{n}\Big)\zeta_5^{(n-1)/5}\,q^{n^2/600} \;+\; \sum_{n\equiv 2 \pmod 5}\Big(\frac{12}{n}\Big)\zeta_5^{-2a(n-7)/5}\,q^{n^2/600}\\ &=\; \zeta_{25}^2\,\eta(\tau)\Big[f\Big(\frac{\tau+2}{5}\Big)^{-1} \;-\; f\Big(\frac{\tau-2}{5}\Big)\Big]\end{aligned}$$

for the theta series of χ_1, while for χ_2 we use $\big(\frac{24}{n}\big)=(-1)^{(n^2-1)/8}\big(\frac{12}{n}\big)$ to get

$$\begin{aligned}\frac{\zeta_{16}}{2}\,\theta(\chi_2,\tau) \;&=\; \sum_{n\equiv 1 \,(5)}\Big(\frac{12}{n}\Big)\zeta_5^{2(n-1)/5}\,\mathbf{e}\big(n^2\,\frac{\tau+75}{1200}\big) \;+\; \sum_{n\equiv 2 \,(5)}\Big(\frac{12}{n}\Big)\zeta_5^{(n-7)/5}\,\mathbf{e}\Big(n^2\,\frac{\tau+75}{1200}\Big)\\ &=\; \zeta_{25}^2\,\eta\big(\frac{\tau+75}{2}\big)\Big[\zeta_{25}^4\,f\Big(\frac{\tau+83}{10}\Big)^{-1} \;-\; \zeta_{25}^{-1}\,f\big(\frac{\tau+77}{10}\big)\Big]\\ &=\; -\zeta_{25}^{-11}\,\eta\big(\frac{\tau+3}{2}\big)\Big[f\Big(\frac{\tau+3}{10}\Big)^{-1} \;-\; f\Big(\frac{\tau-3}{10}\Big)\Big].\end{aligned}$$

(In the last line we used that $\eta(\tau+1)=\zeta_{24}\eta(\tau)$ and $f(\tau+1)=\zeta_5 f(\tau)$.) The vanishing of $\Theta(\chi_1)$ and $\Theta(\chi_2)$ is therefore a consequence of the following evaluations:

Proposition 2. *The values of $f(\tau)$ for $\tau\in\Big\{\frac{i+2}{5},\ \frac{i-2}{5},\ \frac{i+3}{10},\ \frac{i-3}{10}\Big\}$ are given by*

$$f\big(\frac{i\pm 2}{5}\big) \;=\; f\big(\frac{i\mp 3}{10}\big) \;=\; \zeta_{20}^{\pm 1}\,.$$

Proof. Using the well-known (and easily proved) modular identity

$$f(\tau)^{-5} \;-\; f(\tau)^5 \;=\; \left(\frac{\eta(\tau)}{\eta(5\tau)}\right)^6 \;+\; 11\,,$$

together with the transformation formula $\eta(-1/\tau)=(\tau/i)^{1/2}\,\eta(\tau)$ we find

$$f\left(\frac{i\pm 2}{5}\right)^{-5} \;-\; f\left(\frac{i\pm 2}{5}\right)^{5} \;-\; 11 \;=\; \left(\frac{\eta\big(-1/(i\mp 2)\big)}{\eta(i\mp 2)}\right)^6 \;=\; \left(\frac{i\mp 2}{i}\right)^3 \;=\; \mp 2i \;-\; 11$$

and hence $f\big(\frac{i\pm 2}{5}\big)^5=\pm i$, from which the formula for $f\big(\frac{i\pm 2}{5}\big)$ follows by taking fifth roots (the choice of root being determined by a numerical calculation). The calculation for $f\big(\frac{i\pm 3}{10}\big)$ is exactly similar and is left to the reader. $\square$

§3. Proof of Proposition 1

This proposition is essentially a specialization of Watson's quintuple product identity, of which we include a short proof for the sake of completeness. Watson's identity can be found in the literature in a number of equivalent forms, a typical one being

$$\sum_{k=-\infty}^{\infty} \bigl(q^{2k+1}z^2 \,-\, 1\bigr)\, q^{(3k^2+k)/2}\, z^{3k+1} \;=\; (q, z, qz^{-1}; q)_\infty\, (qz^2, qz^{-2}; q^2)_\infty\,, \tag{7}$$

in which the symbol $(x_1, \dots, x_k; q)_\infty$ denotes the product $(x_1; q)_\infty \cdots (x_k; q)_\infty$ with $(x; q)_\infty = \prod_{n=0}^{\infty}(1 - q^n x)$. Before giving the proof, we make a general comment. The literature on q-series abounds with identities of the general form of (7), often far more complicated, in which each term is made up of theta series and infinite products of the form $(q^{\alpha_1}z^{\beta_1}, \dots, q^{\alpha_k}z^{\beta_k}; q)_\infty$, each multiplied by a monomial in q and z. Any such identity can be put into a canonical, and almost always much simpler, form by applying the following two general rules:

(i) "Complete the squares" to write any theta-series $\sum_n c(n)\, q^{Q(n)} z^{L(n)}$, where $c(n)$ is a periodic function of n and $Q(n)$ and $L(n)$ are quadratic and linear in n, respectively, as the product of a monomial in q and z with a "pure" theta series in which Q and L are of the form an^2 and bn, with no lower order terms. For instance, the left-hand side of Euler's identity

$$\sum_{k\in\mathbb{Z}} (-1)^k\, q^{(3k^2+k)/2} \;=\; \prod_{n=1}^{\infty} \bigl(1 - q^n\bigr) \tag{8}$$

should by this rule be multiplied by $q^{1/24}$ to rewrite it as $\sum_n \left(\frac{12}{n}\right) q^{n^2/24}$, in which case the right-hand side becomes the Dedekind eta-function.

(ii) Replace each infinite product by a theta series (possibly multiplied or divided by a product of Dedekind eta functions) by using the Jacobi triple product identity

$$\sum_{n\in\mathbb{Z}} \left(\frac{-4}{n}\right) q^{n^2/8}\, z^{n/2} \;=\; q^{1/8}\, z^{1/2}\, \bigl(q, qz, z^{-1}; q\bigr)_\infty\,. \tag{9}$$

This will always be possible.

When this is done, all monomials in q and z will automatically disappear, since the eta-function and the "pure" theta series are always modular or Jacobi forms (in the variables τ and u, where $q = \mathbf{e}(\tau)$ and $z = \mathbf{e}(u)$) and an identity among such forms cannot involve powers of q or z.

Applying these rules to equation (7), we write the two factors on the right-hand side as $-q^{-1/8}z^{1/2}$ times $\sum_a \left(\frac{-4}{a}\right) q^{a^2/8}\, z^{a/2}$ and $q^{1/12}$ times $\eta(2\tau)^{-1} \sum_b (-1)^b q^{b^2} z^{2b}$, respectively, while the left-hand side becomes $-q^{-1/24}z^{1/2}$ times $\sum_m \left(\frac{-12}{n}\right) q^{n^2/24} z^{n/2}$. (Set $-6k - 5 = n$ in the first term and $6k + 1 = n$ in the second.) The monomials in q and z cancel as promised, and the identity takes on the following form, which is not only considerably less artificial-looking than (7), but also allows an essentially one-line proof, as we will see in a moment.

Proposition 3 ("Quintuple product identity"). *For $\tau \in \mathfrak{H}$, $q = \mathbf{e}(\tau)$ and $z \in \mathbb{C}$ we have*

$$\left(\sum_{n\in\mathbb{Z}} \left(\frac{-12}{n}\right) q^{n^2/24}\, z^{n/2}\right) \eta(2\tau) \;=\; \left(\sum_{a\in\mathbb{Z}} \left(\frac{-4}{a}\right) q^{a^2/8}\, z^{a/2}\right) \left(\sum_{b\in\mathbb{Z}} (-1)^b\, q^{b^2} z^{2b}\right). \tag{10}$$

Proof. From Euler's identity in the form given above we immediately find[2]

$$\left(\frac{-12}{n}\right) \eta(\tau) \;=\; \sum_{\substack{m\in\mathbb{Z} \\ m\equiv n \pmod 6}} \left(\frac{-4}{m}\right) q^{m^2/24} \qquad (n \in \mathbb{Z}) \tag{11}$$

[2]This trick is taken from [5].

(it suffices to check this for $n = 1$ or 2, since both sides are odd and of period 6 in n) and hence

$$\text{LHS of (10)} \;=\; \sum_{\substack{m,\,n\in\mathbb{Z}\\ m\equiv n \pmod 6}} \Big(\frac{-4}{m}\Big)\, q^{(2m^2+n^2)/24}\, z^{n/2} \;=\; \text{RHS of (10)}\,,$$

where the second equality is obtained by substituting $m = a - 2b$, $n = a + 4b$. □

Replacing z by $-z$ in the quintuple product identity, we obtain the equivalent identity

$$\sum_{n\in\mathbb{Z}} \Big(\frac{12}{n}\Big)\, q^{n^2/24}\, z^{n/2} \;=\; q^{1/24}\, z^{-1/2} \prod_{n=1}^{\infty} \frac{(1-q^n)(1-q^{n-1}z^2)(1-q^n z^{-2})}{(1-q^{n-1}z)(1-q^n z^{-1})}\,. \tag{12}$$

Making the substitution $(q, z) \mapsto (q^p, q^a z)$ in this formula and rewriting slightly, we find:

Proposition 4. *Let p be an integer prime to 6. Then for every $a \in \mathbb{Z}/p\mathbb{Z} \smallsetminus \{0\}$ we have*

$$\sum_{n\equiv 6a \pmod p} \Big(\frac{12}{n}\Big)\, q^{n^2/24p}\, z^{n/2p} \;=\; \Big(\frac{12}{\beta}\Big)\, q^{\beta^2/24p}\, z^{\beta/2p}$$
$$\times \prod_{\substack{n>0\\ n\equiv 0 \pmod p}} \big(1-q^n\big) \prod_{\substack{n>0\\ n\equiv \pm a \pmod p}} \big(1-q^n z^{\pm 1}\big)^{-1} \prod_{\substack{n>0\\ n\equiv \pm 2a \pmod p}} \big(1-q^n z^{\pm 2}\big)\,,$$

where β is the number prime to 6 of smallest absolute value in the residue class of $6a \pmod p$.

Proposition 1 now follows by specializing to $p = 5$ and z a 5th root of unity.

§4. Proof of non-vanishing

Of course the proof of non-vanishing simply consists in a systematic computer search. Let us briefly explain the details of this search, which was programmed in GP/Pari by the first author. The point to remember is that, because the series in (3) converges so quickly, we will use far fewer than N values of $\chi(n)$, and therefore have to think about how to compute individual values quickly, rather than storing a complete table and using the periodicity.

For each conductor N, we compute the structure of $(\mathbb{Z}/N\mathbb{Z})^\times$ using the Chinese remainder theorem and a naive search for primitive roots, together with technical data allowing reasonably efficient computation of *discrete logarithms* in that group. If

$$(\mathbb{Z}/N\mathbb{Z})^\times = \bigoplus_{i=1}^{k} C_{d_i}\, \overline{g_i}$$

with $d_{i-1} \mid d_i$ for $i > 1$ we represent any character χ by a k-component vector of integers $(c_1, \dots, c_k)$, such that $\chi(g_i) = \zeta_{d_k}^{c_i}$. The computation of $\chi(n)$ for any n is then done using a naive discrete logarithm method, and the check that χ is primitive and/or even is standard. We then compute the series $\Theta(\chi)$ to 38 decimal digits (calculating $e^{-\pi n^2/2N}$ by the obvious recursion) and look if the result is close to 0. For all conductors that we checked (up to $N = 52100$) we have $|\Theta(\chi)| > 10^{-16}$, so we have no problem recognizing non-vanishing; if we ever did, we would simply redo the computation for the particular character giving a small value, to a much larger accuracy. We did the calculations for both even and odd characters (with $\Theta(\chi)$ defined in the odd case as explained in the remark after Theorem 1), for a total of more than $5 \cdot 10^8$ primitive characters.

The heavily optimized search program took less than two days to run on a four processor CPU (approximately one week total CPU time). As stated in the theorem, the search did not reveal any other examples of vanishing theta values, and their distribution seems to be as could be expected: for instance, the smallest nonzero modulus for even characters is $7.3524 \cdot 10^{-16}$ for conductor $N = 20263$, and for odd characters is $9.6759 \cdot 10^{-14}$ for conductor $N = 34535$.

§5. When is the root number a root of unity?

In the above calculation, one does *not* directly get the values of $W(\chi_1)$ or $W(\chi_2)$ from the formula $W(\chi) = \Theta(\chi)/\Theta(\overline{\chi})$ because both $\Theta(\chi)$ and $\Theta(\overline{\chi})$ are zero in these cases, but of course one can calculate these values directly from the definition (1), and it turns out that in both cases the values are roots of unity:

$$W(\chi_1) \;=\; \mathbf{e}(14/25)\,, \qquad W(\chi_2) \;=\; \mathbf{e}(18/25)\,.$$

This suggests the general question:

When is the root number $W(\chi)$ associated to a primitive character χ of conductor N equal to a root of unity?

Surprisingly, we could not find an explicit answer to this question anywhere, although it can be deduced relatively easily from results in the literature. We therefore include the answer here, without any guarantee that it is new.

Theorem 2. *Let χ be a primitive character. The root number $W(\chi)$ is a root of unity if and only if χ is the product of two primitive characters with coprime conductors N_1 and N_2, where the character of conductor N_1 is real and where N_2 is squarefull (that is, $p \mid N_2$ implies $p^2 \mid N_2$).*

Of course $N_1 = 1$ or $N_2 = 1$ are possible.

Proof. We only give a brief sketch: By looking at valuations at all prime ideals and using the Chinese remainder theorem and the fact that $|W(\chi)| = 1$, it is immediate to reduce to the case where the conductor of χ is a prime power, say p^v. Now a theorem of Odoni [4] which deserves to be better known says that when p is odd and $v \geq 2$ then $W(\chi)$ is a root of unity, given explicitly. It is easy to modify Odoni's proof to prove the same statement (with a slightly different formula for the root of unity) also for $p = 2$. This reduces the proof to the case $v = 1$. In this case, Stickelberger's theorem on the prime decomposition of Gauss sums immediately implies that the only characters χ for which $W(\chi)$ is a root of unity are real characters, proving the result. □

Note that the same question but now for Gauss sums attached to *finite fields* has been answered by Evans [1], and independently by Lemke Oliver [3].

Corollary. *Let $N \geq 1$ be given, $N \not\equiv 2 \pmod 4$. All primitive characters of conductor N have root numbers which are roots of unity if and only if N is squarefull or 3 times a squarefull number.*

Notice that the condition on N is necessary, since there are no primitive characters of conductor congruent to 2 modulo 4.

§6. Remarks on the algebraic part of $\Theta(\chi)$

We remark that in principle the numerical calculations of $\Theta(\chi_1)$ and $\Theta(\chi_2)$ to 10,000 decimal digits mentioned in the introduction almost certainly already suffice to prove the vanishing rigorously. By the theory of complex multiplication, one knows that the modular function $\theta(\chi,\tau)/\eta(\tau)^{1+2\epsilon}$ (with ϵ equal 0 or 1 according to the parity of χ) takes on algebraic values at all quadratic arguments, so that the number

$$A(\chi) \;=\; \frac{\Theta(\chi)}{\Omega^{1+2\epsilon}}\,, \qquad \Omega \;=\; \eta(i) \;=\; 0.768225422326\cdots$$

is algebraic. (The number Ω is equal to $\frac{1}{2}\,\pi^{-3/4}\,\Gamma(1/4)$ by the Chowla-Selberg formula, but this plays no role for us.) Furthermore, CM theory actually gives an algorithm (the Shimura reciprocity

law) to compute this algebraic number. One could therefore in principle estimate the degree, denominator, and height of $A(\chi)$ (roughly speaking, the maximal size of the coefficients of its minimal polynomial over $\mathbb{Q}$) in terms of the size of the conductor, and presumably these estimates in the case of characters of conductor as small as 300 or 600 would be more than sufficient to deduce rigorously the vanishing of $\Theta(\chi_1)$ and $\Theta(\chi_2)$ from their vanishing to 10,000 decimals. We have not carried this out, but did calculate $A(\chi)$ for several characters of small prime conductor p. In this final section we report on our findings. Presumably the results we observe can be proved and generalized to nonprime conductors, and the vanishing of $\Theta(\chi)$ for our two special characters should then follow easily.

First, we noticed that 2 and p are the only primes below the denominator of $A(\chi)$, with the prime 2 occurring only for odd characters. This should be easy to prove. For example, for $p = 7$ and the two conjugate characters of order 3, the numbers $7^3 A(\chi)^{12}$ are roots of an 8th degree polynomial

$$\begin{aligned} 7\,x^8 \;-\; 7\cdot 109044\,x^7 \;+\; 7^2\cdot 492680350\,x^6 \;-\; 7\cdot 89850666672\,x^5 + 12494969491885\,x^4 \\ -\; 7^2\cdot 3^6\cdot 2149780880\,x^3 \;-\; 7^5\cdot 3^{13}\cdot 12682\,x^2 \;+\; 7^6\cdot 3^{18}\cdot 676\,x \;+\; 7^7\cdot 3^{24} \end{aligned}$$

with integral coefficients. In many cases that we checked, we found that the equations become much simpler, and the integrality statement better, if one multiplies $A(\chi)$ by its complex conjugate. Specifically, in the cases checked (all χ with conductor less than 50), the number

$$B(\chi) \;=\; \begin{cases} p\,A(\chi)^2 & \text{if } \chi \text{ is trivial,} \\ 2^\epsilon\sqrt{p}\,|A(\chi)|^2 & \text{if } \chi \text{ is nontrivial,} \end{cases}$$

is an algebraic integer. (Observe that although up to now we have restricted to primitive characters, we now include also the trivial character.) For instance, in the case just given the number $B(\chi) = \sqrt{7}\,|A(\chi)|^2$ is a root of the much simpler polynomial $x^8 + 42x^6 + 119x^4 - 126x^2 - 567$ and is integral, even though, as we just saw, its two factors $7^{1/4}A(\chi)$ and $7^{1/4}\overline{A(\chi)}$ are not individually integers.

Instead of considering the product of $A(\chi)$ just for a given character and its complex conjugate, however, it is much more natural to consider the product of the numbers $A(\chi)$ for *all* characters χ of a given order, since these characters form a Galois orbit and one can reasonably expect that this product, whose vanishing is of course equivalent to that of one of the $\Theta(\chi)$, will belong to a much smaller field. This is indeed what we find. More precisely, for all primes p and all divisors m of $p-1$ we define a (conjecturally integral) algebraic number $N_p(m)$ by

$$N_p(m) \;=\; \prod_{\substack{\chi \text{ of order } m \\ \text{up to } \chi\sim\overline{\chi}}} B(\chi) \;=\; \begin{cases} p\,A(\chi_0)^2 & \text{if } m = 1\,, \\ 2^\epsilon\sqrt{p}\,A\big(\left(\tfrac{\cdot}{p}\right)\big)^2 & \text{if } m = 2\,, \\ \displaystyle\prod_{\chi \text{ of order } m} 2^{\epsilon/2}p^{1/4}\,A(\chi) & \text{if } m \ge 3\,. \end{cases}$$

Then in all cases tested we found that either $N_p(m)$ or its square belonged to the field $L = \mathbb{Q}\big(j(i\,p)\big)$, the real part of the ring class field of discriminant $-4p^2$. (Here j denotes the classical elliptic modular function of level 1.) In many cases, it even turned out that $N_p(m)$ was the square of a number in L.

The data we obtained is summarized in the four tables below, which we include for the benefit of readers who are either simply curious or who want to look for or prove patterns in these numbers. For $p \le 13$, we give an explicit description of the above ring class field L and give for all divisors m of $p-1$ the value of the smallest power $N_p(m)^d$ belonging to L. For larger primes the algebraic numbers become too unwieldy to write down and we give only the norms. All norms are given in factored form. (In these factorizations, C denotes a large composite number and P a large prime, "large" here meaning greater than 200.) We fix the notations $\delta = \sqrt{p}$, $F = \mathbb{Q}(\delta)$ and $L = \mathbb{Q}(j(i\,p))$. For $p = 3$ and $p = 7$ we also use ε to denote a fundamental unit of F.

Here is the table giving the field $\mathbb{Q}(j(i\,p))$ (as well as the value of $j(i\,p)$ itself for $p \le 7$, simply to emphasize how large its coefficients are) for $p < 15$:

p	$L \;=\; \mathbb{Q}(j(i\,p))$	$j(i\,p)$
3	$F \quad (\varepsilon = 2+\delta)$	$192\,(399849 + 230888\,\delta) = 2^6\varepsilon^2\delta^3(20+7\,\delta)^3$
5	F	$6^3\,(2927 + 1323\,\delta)^3$
7	$F(t),\ t = \sqrt{\delta\varepsilon} \quad (\varepsilon = 8 - 3\,\delta)$	$6^3\,(96959 + 36648\,\delta + (238284 + 90063\,\delta)\,t)^3$
11	$F \cdot \mathbb{Q}(u),\ u^3 - u^2 + 4u + 2 = 0$	(31-digit coefficients)
13	$F \cdot \mathbb{Q}(v),\ v^3 - v^2 - 4v + 12 = 0$	(36-digit coefficients)

The corresponding values of $N_p(m)^d$ (= smallest power of $N_p(m)$ belonging to L) are given by

p	m	d	$N_p(m)^d$	Norm
3	1	2	$-3 + 2\delta$	-3
	2	1	δ	-3
5	1	1	$1 + \delta$	-2^2
	2	1	$3 - \delta$	2^2
	4	2	20δ	$-5^3 \cdot 2^4$
7	1	2	$-63 + 36\delta + (58 + 8\delta)\,t$	$-7 \cdot 3^8$
	2	1	$-3\delta + (36 + 14\delta)\,t$	$-7 \cdot 113^2$
	3	2	$(-21 - 6\delta + (50 + 19\delta)\,t)/2$	$-7 \cdot 3^4$
	6	1	$(3\delta + (15 + 4\delta)\,t)/2$	$-7 \cdot 19^2$
11	1	2	$(2519 + 926\delta - (1936 + 144\delta)\,u + (440 + 260\delta)\,u^2)/11$	$-11 \cdot 5^{12}$
	2	1	$(-176 + 59\delta + (66 - 46\delta)\,u - (66 - 14\delta)\,u^2)/11$	$-11 \cdot 3^4 \cdot P^2$
	5	1	$(-517 + 167\delta + (198 - 133\delta)\,u - (55 - 40\delta)\,u^2)/22$	$-11 \cdot 5^3 \cdot P^2$
	10	1/2	$(583 + 43\delta + (33 - 38\delta)\,u - (22 - 13\delta)\,u^2)/22$	$11 \cdot 3^4 \cdot P$
13	1	1	$(325 - 67\delta - (65 + \delta)\,v - (39 - 21\delta)\,v^2)/13$	$-2^6 \cdot 3^6$
	2	1	$(-143 - 47\delta - 4\delta v + (26 + 6\delta)\,v^2)/13$	$2^6 \cdot 3^6$
	3	1	$(52 - 4\delta - (26 - 11\delta)\,v + 3\delta v^2)/26$	$2^2 \cdot 3^7$
	4	2	$-2142 - 458\delta - (252 + 148\delta)\,v + (378 + 130\delta)\,v^2$	$-13^3 \cdot 2^{12} \cdot P^4$
	6	1	$(104 + 8\delta - (39 - 4\delta)\,v + (13 - 6\delta)\,v^2)/26$	$2^2 \cdot 3^2 \cdot 23^2$
	12	1	$-2145 + 376\delta + (78 - \delta)\,v + (195 - 11\delta)\,v^2$	$-13^3 \cdot 2^4 \cdot P^2$

For $15 < p < 50$ the numbers $N_p(m)^d$ become more complicated and we give only the norms.

p	m	d	$N_{L/\mathbb{Q}}\big(N_p(m)^d\big)$
17	1	1	2^{24}
	2	1	$2^{14} \cdot 3^{12}$
	4	1	$2^{10} \cdot 7^4$
	8	1	$2^{20} \cdot 3^4 \cdot 7^4$
	16	1	$17^6 \cdot 2^{20} \cdot C^2$
19	1	2	$-19 \cdot 3^{40}$
	2	1	$-19 \cdot C^2$
	3	2	$-19 \cdot 2^8 \cdot 3^{10} \cdot 47^8$
	6	1	$-19 \cdot 2^2 \cdot 167^2 \cdot P^2$
	9	2	$-19^3 \cdot 3^{10} \cdot 71^4 \cdot P^4$
	18	1	$-19^3 \cdot C^2$
23	1	2	$-23 \cdot 11^{24}$
	2	1	$-23 \cdot 3^4 \cdot C^2$
	11	2	$-23^5 \cdot 11^{12} \cdot P^4$
	22	1	$-23^5 \cdot 43^2 \cdot C^2$
29	1	1	$-2^{14} \cdot 7^{14}$
	2	1	$2^{14} \cdot 3^4 \cdot P^2$
	4	2	$-29^3 \cdot 2^{44} \cdot 7^8 \cdot P^4$
	7	1	$2^6 \cdot 7^9 \cdot 127^4 \cdot 139^2 \cdot P^2$
	14	1	$2^6 \cdot C^2$
	28	1	$-29^9 \cdot 2^{12} \cdot 7^4 \cdot C^2$
31	1	2	$-31 \cdot 3^{32} \cdot 5^{32}$
	2	1	$-31 \cdot 3^2 \cdot C^2$
	3	2	$-31 \cdot 3^{16} \cdot P^4$
	5	1	$-31 \cdot 3^8 \cdot 5^8 \cdot 7^4 \cdot 11^8 \cdot P^2$
	6	1	$-31 \cdot 3^2 \cdot C^2$
	10	1/2	$31 \cdot 3^2 \cdot 7^4 \cdot 11 \cdot C$
	15	1/2	$31 \cdot 2^8 \cdot 3^2 \cdot P$
	30	1/2	$31^2 \cdot 2^8 \cdot 3^2 \cdot 11^2 \cdot P$

p	m	d	$N_{L/\mathbb{Q}}\big(N_p(m)^d\big)$
37	1	1	$-2^{18} \cdot 3^{36}$
	2	1	$2^{18} \cdot 3^4 \cdot C^2$
	3	1	$2^{10} \cdot 3^9 \cdot C^2$
	4	2	$-37^3 \cdot 2^{44} \cdot C^4$
	6	1	$2^{10} \cdot 3^4 \cdot C^2$
	9	1	$2^6 \cdot 3^9 \cdot C^2$
	12	1	$-37^3 \cdot 2^{20} \cdot C^2$
	18	1	$2^6 \cdot 3^8 \cdot 19^4 \cdot C^2$
	36	1	$-37^9 \cdot 2^{12} \cdot 19^4 \cdot 71^2 \cdot C^2$
41	1	1	$2^{40} \cdot 5^{20}$
	2	1	$2^{40} \cdot 103^4 \cdot P^2$
	4	1	$2^{26} \cdot 3^4 \cdot 11^4 \cdot 31^2 \cdot P^2$
	5	1	$2^{16} \cdot 3^{12} \cdot 5^{10} \cdot 7^4 \cdot P^2$
	8	1	$-41^3 \cdot 2^{48} \cdot 3^{16} \cdot 19^4 \cdot P^2$
	10	1/2	$-2^6 \cdot 3^6 \cdot C$
	20	1/2	$2^8 \cdot P$
	40	1/2	$-41^6 \cdot 2^{12} \cdot C$
43	1	2	$-43 \cdot 3^{44} \cdot 7^{44}$
	2	1	$-43 \cdot 3^8 \cdot C^2$
	3	2	$-43 \cdot 2^{16} \cdot 3^{22} \cdot C^4$
	6	1	$-43 \cdot 2^8 \cdot 3^6 \cdot 7^4 \cdot C^2$
	7	2	$-43^3 \cdot 7^{22} \cdot P^4$
	14	1	$-43^3 \cdot C^2$
	21	1	$-43^3 \cdot 2^{12} \cdot C^2$
	42	1/2	$43^3 \cdot 2^6 \cdot 7 \cdot C$
47	1	2	$-47 \cdot 23^{48}$
	2	1	$-47 \cdot 3^4 \cdot 67^2 \cdot C^2$
	23	2	$-47^{11} \cdot 23^{24} \cdot 139^4 \cdot C^4$
	46	1	$-47^{11} \cdot 139^2 \cdot C^2$

The dependence of the exponent d and of the valuation v_p of the norm of $N_p(m)^d$ on the divisor m of $p-1$ becomes more transparent (although still far from completely clear!) if we order the divisors of m lexicographically with respect to $(\ldots, c, b, a)$, where $m = 2^a \cdot 3^b \cdot 5^c \cdot \cdots$. The following table presents the corresponding data (now up to $p = 53$) reorganized in this way.

p	m	d	v_p
3	1 2	2 1	1 1
5	1 2 4	1 1 2	0 0 3
7	1 2 3 6	2 1 2 1	1 1 1 1
11	1 2 5 10	2 1 1 1/2	1 1 1 1
13	1 2 4 3 6 12	1 1 2 1 1 1	0 0 3 0 0 3
17	1 2 4 8 16	1 1 1 1 1	0 0 0 0 6
19	1 2 3 6 9 18	2 1 2 1 2 1	1 1 1 1 3 3
23	1 2 11 22	2 1 2 1	1 1 5 5
29	1 2 4 7 14 28	1 1 2 1 1 1	0 0 3 0 0 9
31	1 2 | 5 10 3 6 | 15 30	2 1 | 1 1/2 2 1 | 1/2 1/2	1 1 | 1 1 1 1 | 1 2
37	1 2 4 3 6 12 9 18 36	1 1 2 1 1 1 1 1 1	0 0 3 0 0 3 0 0 9
41	1 2 4 8 5 10 20 40	1 1 1 1 1 1/2 1/2 1/2	0 0 0 3 0 0 0 6
43	1 2 | 7 14 3 6 | 21 42	2 1 | 2 1 2 1 | 1 1/2	1 1 | 3 3 1 1 | 3 3
47	1 2 23 46	2 1 2 1	1 1 11 11
53	1 2 4 13 26 52	1 1 2 1 1/2 1/2	0 0 3 0 0 9

Here are a few observations concerning the numerical data.

1. The field L contains $F = \mathbb{Q}(\sqrt{p})$ and hence always has even degree. When p is 1 modulo 4, the degree is $n = (p-1)/2$ and the discriminant of L is equal to $(-1)^{(p-5)/4}2^{(p-5)/2}p^{(p-3)/2}$. When p is 3 modulo 4, the degree is $n = (p+1)/2$ and the discriminant is equal to $(-1)^{(p-3)/4}2^{(p+1)/2}p^{(p-1)/2}$. In both cases the Galois closure has degree $2n = p - (-1)^{(p-1)/2}$ and Galois group D_n, the dihedral group of order $2n$.

2. For the trivial character, we observe that we always have $d = 1$ if $p \equiv 1 \pmod 4$ and $d = 2$ if $p \equiv 3 \pmod 4$, with the corresponding norms (here no product is needed, since there is only one trivial character) given by

$$\begin{aligned} N_{L/\mathbb{Q}}\big(B(\chi_0)\big) &= \big(-1\big)^{\frac{p-1}{4}}\,\Big(\frac{p-1}{2}\Big)^{\frac{p-1}{2}} && \text{if } p \equiv 1 \pmod 4, \\ N_{L/\mathbb{Q}}\big(B(\chi_0)^2\big) &= \quad -p\,\Big(\frac{p-1}{2}\Big)^{p+1} && \text{if } p \equiv 3 \pmod 4. \end{aligned}$$

This should be easy to prove.

3. For the Legendre character (the case $m = 2$), we always find $d = 1$ and the same value of v_p as for the trivial character (i.e., 0 or 1 depending on p modulo 4), and the value of $N_p(m)$ divided by this power of p is always a perfect square.

4. More generally, we see in the tables that, up to powers of p and of the prime divisors of m, the norm of $N_p(m)^d$ is always a $(2d)$-th power. A separate computation shows that actually a stronger statement is true, namely, that the ideal generated by $N_p(m)^d$, again up to (ideal) prime factors if pm, is always the $(2d)$-th power of an integral ideal of L. However, by using the structure of the class group we ruled out the stronger possible statement that $N_p(m)$ itself has a factorization as x^2y where x and y^d both belong to L and the latter involves only prime factors of p and m in its factorization.

5. In the final table, where we have given the value of d and v_p in the form of matrices (or of "three-dimensional matrices" in the cases $p = 31$ and $p = 43$ where $p - 1$ has 3 prime factors), we see that the various rows of these matrices are often nearly proportional, i.e., that the various prime factors of $p - 1$ have somewhat independent effects. In the case of the v_p matrix, the correlation of the various rows is even stronger and with the single exception of the value for $p = 31$ and $m = 30$ these matrices always have rank 1.

6. We defined the numbers $B(\chi)$ by including the smallest powers of 2 and p which universally suffice to ensure their integrality, and then $N_p(m)$ as the product of the $B(\chi)$. But in this product one can sometimes change the powers of $2^{1/2}$ or $p^{1/4}$ or both in such a way as to lower the value of the minimal power d that belongs to L. For instance, we have $N_{19}(3)^2 \in L$ and $N_{19}(3) \notin L$, but $2^{1/2}19^{1/4}N_{19}(3) \in L$, and similarly $N_{43}(14) \in L$, $N_{43}(14)^{1/2} \notin L$ but $2^{1/2}N_{43}(14)^{1/2} \in L$. However, there did not seem to be any clear pattern in these modified minimal exponents, so we do not include a table of their values.

7. The final observation concerns the numbers $A(\chi)$ themselves, rather than just the products $B(\chi)$ and $N_p(m)$ that we have been discussing so far. In the example for $p = 7$, $m = 3$ given at the beginning of this section, we saw that $A(\chi)$ was an algebraic number of degree 96, but that its 12th power had degree only 8. This phenomenon of the degree dropping drastically when one takes a power also occurs for other primes, and in fact much more is true. In the example just mentioned, for instance, $A(\chi)^{12}$ not only has degree 8, but belongs to the composite of the two fields $L = \mathbb{Q}(t)$ and $\mathbb{Q}(\zeta_3)$, and is in fact a product of highly factored numbers belonging to these fields, namely

$$7^3 \cdot A(\chi)^{12} \;=\; \varepsilon_1 \cdot \pi_7^{-1} \cdot \pi_3^6 \cdot P_7^2 \quad \in \; L(\zeta_3)\,,$$

where ε_1 is a unit of L (actually, an element of $\mathcal{O}_F^\times\,(\mathcal{O}_L^\times)^6$) and

$$\pi_3 = 2+\delta \in \mathcal{O}_F\,, \qquad \pi_7 = t = \sqrt{\delta\varepsilon} \in \mathcal{O}_L\,, \qquad P_7 = 2+\zeta \in \mathbb{Z}[\zeta_3]$$

are primes with the indicated norms in their respective fields, the value of $\zeta = \zeta_3^{\pm 1}$ being fixed by $\chi(3) = \zeta$. (Here we have included the factor 7^3 on the left to show how it happens that the absolute value of $7^3 A(\chi)^{12}$ is an integer, even though the number itself is not.) The situation for the two characters of conductor 7 and order 6 is very similar: here

$$2^6 \cdot 7^2 \cdot A(\chi)^6 \;=\; \varepsilon^{-2} \cdot \pi_7 \cdot \pi_2^6 \cdot \pi_{19}^6 \cdot P_7^2 \quad \in \; L(\zeta_3)\,,$$

with primes $\pi_2 = 3+\delta \in \mathcal{O}_F$, $\pi_{19} = 12+(t-9\delta)/2 \in \mathcal{O}_L$ and the same prime $P_7 = 3+\zeta \in \mathbb{Z}[\zeta_6]$ as before (but with ζ now fixed by $\chi(2) = \zeta$). For the previous prime $p = 5$ and $m = 4$ (we can now restrict to $m > 2$, since for $m \le 2$ the numbers $A(\chi)$ are essentially the same as $N_p(m)$ and have already been discussed), the situation is even simpler: one has $A(\chi)^4 = P_5 = 1+2i \in \mathbb{Q}(\zeta_4)$. For the next larger prime $p = 11$ and characters of order 5 or 10, the situation becomes more complicated. In these cases some power of $A(\chi)$ again belongs to the composite of L and the cyclotomic field $\mathbb{Q}(\zeta_m)$, but they are no longer products of numbers belonging to these two fields. They are, however, products of a number in $L_1 = L(\sqrt{5})$ and a number in $\mathbb{Q}(\zeta_5)$, with the latter involving only prime factors of p, namely:

$$11^8 \cdot A(\chi)^{20} \;=\; \varepsilon_2^5 \cdot \pi_{11}^5 \cdot \pi_{125}^5 \cdot \pi_{439}^{20} \cdot \alpha^2$$

for the characters of order 5, where ε_2 is a unit of $\mathbb{Q}(\sqrt{55})$, $\pi_{11} \in \mathcal{O}_L$, $\pi_{125} \in \mathcal{O}_L$ and $\pi_{439} \in \mathcal{O}_{L_1}$ are primes of the indicated norms in these fields and α is an element of $\in \mathbb{Z}[\zeta_5]$ with $\alpha \cdot \bar{\alpha} = 11^3$ (more precisely, $\alpha = P_{11,1}^2 \overline{P}_{11,1} P_{11,2}^3$, where the $P_{11,i}$ are primes of norm 11 in $\mathbb{Z}[\zeta_5]$), and

$$2^{5/2} \cdot 11^2 \cdot A(\chi)^5 \;=\; \varepsilon_3 \cdot \pi_{11} \cdot \Pi_{11}^3 \cdot (\Pi_{9,1}\Pi_{9,2}\Pi_{623431})^5 \cdot \beta^2$$

for the characters of order 10, where $\varepsilon_3 \in \mathcal{O}_{L_1}^\times$, $\pi_{11} \in \mathcal{O}_L$ is as before, Π_{11} is one of the two primes above π_{11} in L_1, $\Pi_{9,i}$ and Π_{623431} are primes of these norms in L_1, and β is an element of $\mathbb{Z}[\zeta_5]$ with $\beta\overline{\beta} = 11$ (more precisely, $\beta = P_{11,1}^2 P_{11,2}$). Similar phenomena happen also for larger primes, e.g. for $p = 13$ and $m = 6$ we find $13^{5/2} A(\chi)^6 = c^3(1+3\zeta_6)^2$ with $c \in \mathcal{O}_L$ of norm $(2\cdot 3\cdot 23)^2$, and for $p = 13$ and $m = 4$ we find $13A(\chi)^4 = d^4(2i-3)$ with $d \in \mathcal{O}_L$ of norm 727. We have not been able to do enough computations to make a precise general conjecture, but in any case it seems clear that one always has $A(\chi)^k \in L(\zeta_m)$ for some $k \in \mathbb{N}$ and that $A(\chi^s)^k = \sigma_s(A(\chi)^k)$ for all $s \in (\mathbb{Z}/m\mathbb{Z})^\times$, where σ_s is the element of $\mathrm{Gal}(L(\zeta_m)/L)$ sending ζ_m to ζ_m^s.

References

[1] R. J. Evans, *Generalizations of a theorem of Chowla on Gaussian sums.* Houston J. Math. **3** (1977), 343–349.

[2] S. Louboutin, *Sur le calcul numérique des constantes des équations fonctionnelles des fonctions L associées aux caractères impairs.* C.R. Acad. Sci. Paris **329** (1999), 347–350.

[3] R. Lemke Oliver, *Gauss sums over finite fields and roots of unity.* Proc. Amer. Math. Soc. **139** (2011), no. 4, 1273–1276.

[4] R. Odoni, *On Gauss sums* (mod p^n), $n \ge 2$. Bull. London Math. Soc. **5** (1973), 325–327.

[5] V. Gritsenko, N. Skoruppa, D. Zagier, *Theta blocks.* In preparation.