ACTA ARITHMETICA
145.1 (2010)

Multiplicity results for the functional equation of the Dirichlet L-functions

by

G. Molteni (Milano)

1. Introduction. Let χ be a primitive character modulo q. In [5], the set $W(\chi)$ of Dirichlet series $F(s) := \sum_{n=1}^{\infty} a(n) n^{-s}$ satisfying the following axioms has been introduced:

(i) the coefficients $a(n)$ satisfy the bound $a(n) \ll_\varepsilon n^\varepsilon$ for every $\varepsilon > 0$ and $(s-1)^m F(s)$ admits a continuation to $\mathbb{C}$ as an entire function of finite order for some integer $m \geq 0$;

(ii) $\log F(s)$ is a Dirichlet series whose coefficients $b(n)$ are supported on prime powers, and satisfy the bound $b(n) \ll n^\theta$ for some $\theta < 1/2$;

(iii) $F(s)$ satisfies the functional equation

$$\left(\frac{q}{\pi}\right)^{s/2} \Gamma\left(\frac{s+a(\chi)}{2}\right) F(s) = \frac{\tau(\chi)}{i^{a(\chi)}\sqrt{q}} \left(\frac{q}{\pi}\right)^{(1-s)/2} \Gamma\left(\frac{1-s+a(\chi)}{2}\right) \overline{F(1-\overline{s})}, \tag{1}$$

where $a(\chi) := (1-\chi(-1))/2$ and $\tau(\chi)$ are the parity and the Gauss sum of χ, respectively.

The characterization of the set $W(\chi)$ has been the subject of intensive research, with fundamental contributions by Bochner [2], Vignéras [15], Gérardin & Li [4], Piatetski-Shapiro & Raghunathan [13] and Kaczorowski & Perelli [6]. These authors all prove, with different technics and different generality, that $W(\chi)$ coincides with the set of Dirichlet L-functions $L(s,\psi)$ associated with characters ψ with $a(\psi) = a(\chi)$ and $\tau(\psi) = \tau(\chi)$. According to the definition we will introduce below, this means that $W(\chi)$ coincides with the set of Dirichlet L-functions which are associated with characters having the same signature of χ. The set of conductors q for which $L(s,\chi)$ is

2010 *Mathematics Subject Classification*: Primary 11M06; Secondary 11L05.
Key words and phrases: Gauss sums, functional equations in degree one.

DOI: 10.4064/aa145-1-3

the unique solution in $W(\chi)$ of (1) has been completely determined in [5] and coincides essentially with the set of squarefree integers (some repeated factors are allowed at primes 2 and 3). Thus, for non-squarefree conductors the computation of $|W(\chi)|$ is a non-trivial problem and the present paper accomplishes this task for integers which are either an odd prime power, or whose prime factors have the following property:

$(*)$ $\quad (p\varphi(p), p'\varphi(p')) = 2$ for any distinct primes p, p' dividing q.

Such a strong requirement comes from the fact that it allows us to decompose the problem for composite q into a collection of simpler subproblems for prime power conductors, which is the case to which our approach is particularly well tuned. Hence, the motivation for $(*)$ is essentially technical, nevertheless at present we do not see how to relax it and probably a new idea is needed to solve the problem in greater generality.

We now give a quick overview of our results. In Theorem 1 we find formulæ for the cardinality of $W(\chi)$ and of the analogous set $T(\chi) := \{\psi : \tau(\psi) = \tau(\chi)\}$, in terms of some parameters associated with the character χ, when q is an odd prime power. With a bit of extra work (Propositions 3–4) these parameters become explicitly and easily computable. Theorems 5 and 6 contain similar results for composite integers satisfying $(*)$.

Theorem 3 (for prime powers) and Theorem 7 (for numbers satisfying $(*)$) compute the number of distinct values of the Gauss sum and the number of distinct signatures; the latter number is quite interesting since it counts the functional equations of type (1) and conductor q having non-trivial solutions. By the work of Kaczorowski & Perelli [6] this set coincides with the set of admissible functional equations of degree 1 and conductor q in the Selberg class.

Also some qualitative information is deduced, for example that for the integers considered here $|W(\chi)| = O_\varepsilon(q^{1/2+\varepsilon})$, and that this bound is essentially optimal since $|W(\chi)| \gg \sqrt{q}$ for suitably chosen characters χ modulo q and infinitely many integers q. The smallest value of $|W(\chi)|$ is also of interest. Apart from the prime $p = 3$ which in this respect is exceptional, for the other odd primes we find that $W(\chi) \geq 2$ whenever $q = p^k$ with $k \geq 4$, with 2 as the most probable value for $W(\chi)$ in a statistical sense which is explained in Proposition 5. This means that for a generic character χ modulo p^k (p odd, $k \geq 4$) its functional equation (1) has a large probability to have exactly two solutions. On the contrary, when the conductor is of the form p^k with $k \leq 3$ there are still characters χ for which $|W(\chi)| = 1$, i.e., functional equations of type (1) having a unique solution. These characters can be determined and enumerated explicitly.

In this paper only odd primes are considered. In fact, the analogous problem for $q = 2^k$ can be tackled along similar lines and produces similar

conclusions, but the different structure of the group $\mathbb{Z}_{2^k}^*$ is reflected in several technical differences, and we prefer to leave the presentation of those results to a separate paper [10].

The paper is organized as follows: in Section 2 we recall some facts to fix our notation and we give the definitions of some new objects; in Section 3 we prove our main results and several consequences for odd prime powers; and in Section 4 we prove results for composite conductors.

2. Definitions and preliminary facts

2.1. Gauss sums. Given an integer q, a character χ modulo q and a primitive qth root ζ_q of unity, the Gauss sum $\tau(\chi,\zeta_q)$ is defined as $\tau(\chi,\zeta_q) := \sum_{n=1}^{q}\chi(n)\zeta_q^n$. It depends not only on the character χ but also on the root ζ_q according to the relation

$$\chi(b)\tau(\chi,\zeta_q^b) = \tau(\chi,\zeta_q) \quad \forall b : (b,q) = 1.$$

For convenience, we denote by $\tau(\chi)$ the Gauss sum $\tau(\chi, e(1/q))$. The Gauss sum is a multiplicative map when considered as a function of both χ and ζ; in fact, let q_1 and q_2 be coprime integers, χ_1, χ_2 be primitive characters modulo q_1, q_2 respectively, and ζ_{q_1}, ζ_{q_2} be primitive roots of unity of order q_1 and q_2, respectively. Then $\tau(\chi_1\chi_2,\zeta_{q_1}\zeta_{q_2}) = \tau(\chi_1,\zeta_{q_1})\tau(\chi_2,\zeta_{q_2})$. Explicit formulæ for Gauss sums modulo squarefull prime powers have been found by Odoni [12] for odd primes and extended to the prime 2 by Funakura [3]; an alternative proof has been given by Mauclaire [8, 9] (see also [1]).

2.2. Groups $\mathbb{Z}_{p^k}^*$, p odd prime. The group $\mathbb{Z}_{p^k}^*$ is cyclic. Let $U_k := \{x \in \mathbb{Z}_{p^k}^* : x^{p-1} = 1\}$ and $V_k := \{x \in \mathbb{Z}_{p^k}^* : x^{p^{k-1}} = 1\}$. Then $|U_k| = p-1$, $|V_k| = p^{k-1}$ and $\mathbb{Z}_{p^k}^*$ is the direct product of U_k and V_k. The map $U_k \to \mathbb{Z}_p^*$ associating with $x \in U_k$ its class modulo p is a group isomorphism, thus for every integer z the congruence $x = z \pmod p$ has a solution $x \in U_k$ if and only if $p \nmid z$ and in this case the solution is unique. Let g be a primitive root modulo p^k. Each character χ modulo p^k is determined by the integer α_χ, unique modulo $\varphi(p^k)$, such that $\chi(g) = e(\alpha_\chi/\varphi(p^k))$, and χ is even if and only if α_χ is even, and primitive if and only if p does not divide α_χ. The decomposition $\mathbb{Z}_{p^k}^* = U_k \times V_k$ reflects in a decomposition of each character χ of $\mathbb{Z}_{p^k}^*$ as the product of a character χ_U of U_k and a character χ_V of V_k. According to this decomposition, χ is primitive if and only if among the values of χ_V there are primitive p^{k-1}th roots of unity, and χ is even if and only if $\chi_U(-1) = 1$.

2.3. Signatures. Let χ be a primitive character modulo q and let $a(\chi)$ denote its parity. Let ζ_q be a primitive qth root of unity. The *signature* of χ at ζ_q is the couple of data $(a(\chi),\tau(\chi,\zeta_q))$ and we denote it by $s(\chi;\zeta_q)$;

$s(\chi)$ abbreviates $s(\chi; e(1/q))$. By abuse of notation, we denote by $W(\chi)$ also the set $\{\psi : s(\psi) = s(\chi)\}$; analogously, we denote by $T(\chi)$ the set $\{\psi : \tau(\psi) = \tau(\chi)\}$.

2.4. Three arithmetical functions. We denote by Ψ the multiplicative function whose values at a prime power p^k with $k > 0$ are defined as follows:

$$\Psi(p^k) := \begin{cases} 1 & \text{if } k \in \{1, 2\}, \\ 2 \cdot 3^{k-3} & \text{if } k \geq 3 \text{ and } p = 3, \\ 1 + \dfrac{p^{k-1} - p^{\delta}}{2(p+1)} & \text{if } k \geq 3 \text{ and } p \geq 5, \text{ with } \delta \in \{0, 1\} \\ & \text{and } \delta + k = 1 \pmod 2. \end{cases}$$

The values of Ψ at the 2-powers are not defined since they will not be used in this paper; conventionally we set them to 1. Moreover, we denote by Φ the multiplicative function $\Phi(n) := \sum_{d|n} d\varphi(d)$ and by Φ^* the function $\Phi^*(n) := \sum_{d|n} d^*\varphi(d)$, where $d^* := d$ if d is even, $d^* := 2d$ if d is odd. Writing n as $2^N m$ with m odd, we see that

$$\begin{aligned} \Phi^*(n) &= \sum_{d|n} d^*\varphi(d) = \sum_{d|n} d\varphi(d) + \sum_{\substack{d|n \\ d \,\text{odd}}} d\varphi(d) \\ &= (1 + \Phi(2^N))\Phi(m) = \Phi^*(2^N)\Phi(m). \end{aligned} \tag{2}$$

2.5. Invariants associated with a character. Let p be an odd prime, and let $k > 1$. Let g be a primitive root modulo p^k and let r be an integer coprime to p such that $g^{p-1} = 1 + rp \pmod{p^2}$. Let χ be a primitive character modulo p^k, with $\chi(g) = e(\alpha_\chi/\varphi(p^k))$. The number α_χ is coprime to p and there exists a unique $u \in U_k$ satisfying $ur = -\alpha_\chi \pmod p$. Both r and α_χ depend on g, but u is g-independent; we denote it by u_χ and by d_χ its order in U_k. The number $1 + p$ generates V_k, hence there exists an integer a_χ (unique modulo p^{k-1}) such that $\chi(1 + p) = e(-a_\chi/p^{k-1})$. The integer r is determined only modulo p, but the integer $(1 + p)^{p^{k-2}r}$ is well defined modulo p^k with value $1 + rp^{k-1}$, and

$$e(-a_\chi r/p) = \chi((1 + p)^{p^{k-2}r}) = \chi(1 + rp^{k-1}).$$

Moreover, the definition of r implies that $g^{p^{k-2}(p-1)} = 1 + rp^{k-1} \pmod{p^k}$ and we have

$$e(-a_\chi r/p) = \chi(1 + rp^{k-1}) = \chi(g^{(p-1)p^{k-2}}) = e(\alpha_\chi/p)$$

so that $a_\chi r = -\alpha_\chi \pmod p$, proving that $a_\chi = u_\chi \pmod p$. Hence, there exists an integer z (unique modulo p^{k-2} and independent of g) such that $a_\chi = u_\chi(1 + zp) \pmod{p^{k-1}}$; we denote this integer by z_χ. Finally, we remark that the couple (u_χ, z_χ) uniquely determines the component χ_V of χ, because

the couple determines a_χ which gives the value of χ at the generator $1+p$ of V_k.

2.6. A special p-adic function. Let w be the p-adic function

$$w(z) := \frac{\log(1+zp)}{\log(1+p)}.$$

The power series defining $w(z)$ converges p-adically for every p-adic integer z. In particular, for every such z we have $(1+p)^{w(z)} = 1+zp$ and

$$w'(z) = \frac{p}{(1+pz)\log(1+p)}.$$

Moreover, let C_p be the p-adic integer

$$C_p := \frac{1-\log(p/\log(1+p))}{\log(1+p)} - \frac{1}{p},$$

and finally for $z \in \mathbb{Z}_p$ let F denote the p-adic function

$$F(z) := \frac{z-w(z)}{p} - z(w(z)-C_p).$$

Reducing $F(z)$ modulo p we get

$$F(z) = \begin{cases} \frac{p-1}{2}(z^2+z) \pmod p & \text{if } p>3, \\ 2z+z^2+2z^3 \pmod 3 & \text{if } p=3. \end{cases} \tag{3}$$

The function F inherits from w a representation as power series that converges for every p-adic integer. A simple computation shows that

$$F'(z) = -w(z) - \frac{\log(p/\log(1+p))}{\log(1+p)},$$

implying that $F'(z)=0$ at the unique p-adic integer

$$z_0 := \frac{\log(1+p)-p}{p^2}. \tag{4}$$

Note that $z_0 = \frac{p-1}{2} \pmod p$ for every $p>3$, but $z_0 = 2 \pmod 3$ for $p=3$. Finally, we remark that $F''(z) = -w'(z) = -1 \pmod p$ and $F'''(z) = -w''(z) = 0 \pmod p$ for every p-adic integer z.

3. Main results. As we have anticipated in the Introduction, the main theme of this paper is the study of the set $W(\chi)$ of characters having the same signature as χ. This set is evidently strictly related with the set $T(\chi)$ of characters having the same Gauss sum as χ, and for the moment we concentrate on this second set. In Section 4 we shall see that there is a procedure, based upon the multiplicativity of the Gauss sum, reducing the problem for a composite q to a collage of similar results for the prime power dividing q. Nevertheless, we shall see that in order to take advantage of

this approach the problem must be generalized as follows: determine the characters ψ for which $\tau(\chi) = \vartheta\tau(\psi)$ and $\vartheta \in \{\pm 1\}$, for every given character χ modulo q when q is a prime power. The case $\vartheta = 1$ corresponds to the original problem, and the case $\vartheta = -1$ is introduced only as a tool for Section 4. Concluding, in this section q always denotes an odd prime power p^k and we study equalities of the form $\tau(\chi) = \vartheta\tau(\psi)$ with $\vartheta \in \{\pm 1\}$. The next result shows that this equality admits only the trivial solution when q itself is a prime. The statement of the proposition is slightly more general than what we need here, because a generic root of unity ϑ is admitted; we formulate it in the present form for a possible future reference.

PROPOSITION 1. *Let p be an odd prime and let χ, ψ be primitive characters modulo p. Let ζ_p be a primitive pth root of unity. Suppose that $\tau(\chi, \zeta_p) = \vartheta\tau(\psi, \zeta_p)$ where ϑ is any root of unity. Then $\chi = \psi$.*

Proof. Let K^0 and K be the cyclotomic fields $\mathbb{Q}[e(1/\varphi(p))]$ and $\mathbb{Q}[e(1/p), e(1/\varphi(p))]$, respectively. For every a coprime to p there exists a Galois automorphism $\sigma_a \in \mathrm{Gal}(K/K^0)$ such that $\sigma_a(e(1/p)) = e(a/p)$, hence

$$\sigma_a(\tau(\chi, \zeta_p)) = \tau(\chi, \zeta_p^a) = \overline{\chi(a)}\,\tau(\chi, \zeta_p),$$

implying that

$$\chi(a) = \frac{\tau(\chi, \zeta_p)}{\sigma_a(\tau(\chi, \zeta_p))}.$$

The equality $\vartheta = \tau(\chi, \zeta_p)/\tau(\psi, \zeta_p)$ shows that $\vartheta \in K$ so that ϑ is a $\varphi(p^2)$th root of unity. Let $\vartheta = \vartheta_{p-1}\vartheta_p$ be the decomposition into a product of a $(p-1)$th root and a pth root of unity. Then $\sigma_a(\vartheta_{p-1}) = \vartheta_{p-1}$ and $\sigma_a(\vartheta_p) = \vartheta_p^a$ so that

$$\begin{aligned} \chi(a) &= \frac{\tau(\chi, \zeta_p)}{\sigma_a(\tau(\chi, \zeta_p))} = \frac{\vartheta_{p-1}\vartheta_p\tau(\psi, \zeta_p)}{\sigma_a(\vartheta_{p-1}\vartheta_p\tau(\psi, \zeta_p))} \\ &= \frac{\vartheta_p}{\vartheta_p^a}\,\frac{\tau(\psi, \zeta_p)}{\sigma_a(\tau(\psi, \zeta_p))} = \vartheta_p^{1-a}\psi(a). \end{aligned} \tag{5}$$

Since χ/ψ is a character modulo p, the above identity implies that $\vartheta_p^{1-ab} = \vartheta_p^{1-a}\vartheta_p^{1-b}$ for every $a, b \in \mathbb{Z}_p^*$. This is impossible if $\vartheta_p \neq 1$, hence $\vartheta_p = 1$ and $\chi = \psi$ by (5). ∎

By Proposition 1 we can assume from now on that q is a squarefull prime power so that we have at our disposal Odoni's formula for the value of a Gauss sum. We recall it in the form given by Funakura in [3].

THEOREM (Odoni–Funakura). *Let $q = p^k$ with p odd prime and $k > 1$. Let χ be a primitive character modulo q. Then*

$$\frac{\tau(\chi)}{\sqrt{q}} = \varepsilon_\chi \chi(a_\chi) e(a_\chi(1 + pC_p)/q)$$

where

$$\varepsilon_\chi := \begin{cases} 1 & \text{if } k \text{ is even,} \\ \left(\dfrac{a_\chi}{p}\right) i^{(1-p)/2} & \text{if } k \text{ is odd.} \end{cases}$$

Using this result we prove the following proposition characterizing the characters χ, ψ modulo q having equal Gauss sums, in terms of their parameters u_χ, u_ψ, z_χ, z_ψ and of the function F.

PROPOSITION 2. *Let $q = p^k$ with p odd prime and $k > 1$, let χ, ψ be primitive characters modulo p^k, and let $\vartheta \in \{\pm 1\}$. Then*

$$(6)\quad \tau(\chi) = \vartheta\tau(\psi) \quad \text{if and only if} \quad \begin{cases} \text{(6.a) } u_\chi = u_\psi =: u, \\ \text{(6.b) } \chi(u) = \vartheta\psi(u), \\ \text{(6.c) } F(z_\chi) = F(z_\psi) \pmod{p^{k-2}}, \end{cases}$$

where the last condition is significant only if $k \geq 3$.

Proof. Assume that $\tau(\chi) = \vartheta\tau(\psi)$, so that

$$(7)\qquad \varepsilon_\chi \chi(a_\chi) e(a_\chi(1 + pC_p)/q) = \vartheta\varepsilon_\psi\psi(a_\psi)e(a_\psi(1 + pC_p)/q)$$

by Odoni's result. Taking the $\varphi(q)$th power of this identity we deduce that

$$e(a_\chi(p-1)/p) = e(a_\psi(p-1)/p)$$

(because $\chi(a_\chi)$ and $\psi(a_\psi)$ are $\varphi(q)$th roots of unity, $\vartheta^2 = 1$ and $\varepsilon_\chi^2 = \varepsilon_\psi^2$), thus $a_\chi = a_\psi \pmod p$ implying $u_\chi = u_\psi$, which is (6.a). Let u denote this common value. The Legendre symbol $\left(\frac{\cdot}{p}\right)$ depends only on the class modulo p so that $\left(\frac{a_\chi}{p}\right) = \left(\frac{u}{p}\right) = \left(\frac{a_\psi}{p}\right)$ and, under (6.a), the equality in (7) can be written as

$$\chi(a_\chi)e(a_\chi(1 + pC_p)/q) = \vartheta\psi(a_\psi)e(a_\psi(1 + pC_p)/q).$$

Introducing the parameters z_χ and z_ψ, and using (6.a), the previous equality becomes

$$(8)\qquad \chi(u(1 + z_\chi p))e(uz_\chi p(1 + pC_p)/q) = \vartheta\psi(u(1 + z_\psi p))e(uz_\psi p(1 + pC_p)/q).$$

The p^{k-1}th power of (8) gives

$$\chi(u(1 + z_\chi p))^{p^{k-1}} = \vartheta\psi(u(1 + z_\psi p))^{p^{k-1}},$$

implying that $\chi(u) = \vartheta\psi(u)$, because $(1 + z_\chi p)^{p^{k-1}} = 1$ in $\mathbb{Z}_q^*$ and $u \in U_k$ implies that $u^p = u$. Hence also the second condition (6.b) is proved. Under (6.a)–(6.b), equality (8) becomes

$$(9)\quad \chi(1 + z_\chi p)e(uz_\chi(1 + pC_p)/p^{k-1}) = \psi(1 + z_\psi p)e(uz_\psi(1 + pC_p)/p^{k-1}).$$

The p-adic map w gives $(1 + p)^{w(z)} = 1 + zp$ so that

$$\chi(1 + z_\chi p) = e(-a_\chi w(z_\chi)/p^{k-1})$$

and (9) becomes

$$-a_\chi w(z_\chi) + uz_\chi(1+pC_p) = -a_\psi w(z_\psi) + uz_\psi(1+pC_p) \pmod{p^{k-1}}.$$

Recalling that $a_\chi = u(1+z_\chi p)$ and $a_\psi = u(1+z_\psi p)$ (by (6.a)), we deduce that $uF(z_\chi) = uF(z_\psi) \pmod{p^{k-2}}$, which is equivalent to (6.c) because u is coprime to p. Each step in the previous argument can be reversed, so that under conditions (6.a)–(6.c) we have $\tau(\chi) = \vartheta\tau(\psi)$. ∎

In view of the previous result, for every given z' we denote by $n_k(z')$ the number of solutions of the congruence

$$F(z) = F(z') \pmod{p^k}. \tag{10}$$

This definition does not apply when $k = 0$: for later use it is useful to set $n_0(z') = 1$ for every z'.

THEOREM 1. *Let $q := p^k$ with p odd prime. Let χ be a primitive character modulo q. Recall that d_χ is the order of u_χ in U_k. Then $|T(\chi)| = (p-1)n_{k-2}(z_\chi)/d_\chi$ and $|W(\chi)| = (p-1)n_{k-2}(z_\chi)/d^*_\chi$, where*

$$d^*_\chi = \begin{cases} d_\chi & \text{if } d_\chi \text{ is even,} \\ 2d_\chi & \text{if } d_\chi \text{ is odd.} \end{cases}$$

Proof. Formula for $|T(\chi)|$. Let ψ be a primitive character modulo p^k. By Proposition 2 we know that $\tau(\psi) = \tau(\chi)$ if and only if (6.a)–(6.c) are satisfied. We have already noticed that the parameters u_ψ and z_ψ uniquely determine ψ_V: by (6.a), u_ψ is fixed, and by (6.c), z_ψ can be chosen in $n_{k-2}(z_\chi)$ ways, therefore there are $1 \cdot n_{k-2}(z_\chi)$ possible couples of data (u_ψ, z_ψ), i.e. of possible ψ_V. The decomposition $\mathbb{Z}^*_{p^k} = U_k \times V_k$ shows that (6.b) is actually a condition for the values that ψ_U assumes on the subgroup of U_k generated by u_χ. As U_k is cyclic, there are $|U_k|/d_\chi = (p-1)/d_\chi$ characters of U_k having a prescribed value at u_χ, so that we have $(p-1)/d_\chi$ possible choices for ψ_U. Hence, we have $(p-1)n_{k-2}(z_\chi)/d_\chi$ possible choices for the couple (ψ_U, ψ_V), i.e. for ψ.

Formula for $|W(\chi)|$. We notice that ψ and χ have the same parity iff $\psi_U(-1) = \chi_U(-1)$, so that ψ has the same signature as χ iff both the equality $\psi_U(-1) = \chi_U(-1)$ and conditions (6.a)–(6.c) are satisfied. The condition on the parity and (6.b) show that the values of ψ_U on the group $\langle -1, u_\chi \rangle$ are fixed by χ. If d_χ is even, from $u_\chi^{d_\chi} = 1$ we get $u_\chi^{d_\chi/2} = -1$ (because d_χ is the order of u_χ), thus -1 belongs to the subgroup generated by u_χ and by (6.b) we conclude that each character satisfying (6.a)–(6.c) already has the same parity as χ. In this case the number of distinct signatures is equal to the number of distinct Gauss sums. If d_χ is odd then -1 does not belong to the group generated by u_χ, and $\langle u_\chi \rangle$ is a subgroup of index 2 in $\langle -1, u_\chi \rangle$, therefore there are only $(p-1)/2d_\chi$ possible choices for ψ_U. Since

as in the previous case we have $n_{k-2}(z_\chi)$ possible choices for ψ_V, the claim follows. ∎

The case $\tau(\psi) = -\tau(\chi)$ is analogous, but presents one difference. Consider (6) with $\vartheta = -1$ and let the order d of u be odd. Then from (6.b) we have the contradiction $1 = \chi(u^d) = \chi(u)^d = -\psi(u)^d = -\psi(u^d) = -1$. It is easy to prove that this is the unique obstruction to the existence of solutions of the system in (6), and the argument we have already used to prove Theorem 1 allows us also to prove the following result.

THEOREM 2. *Let $q := p^k$ with p odd prime. Let χ be a primitive character modulo q. The number of primitive characters ψ modulo q with $\tau(\psi) = -\tau(\chi)$ is 0 if d_χ is odd, and $(p-1)n_{k-2}(z_\chi)/d_\chi$ if d_χ is even.*

Theorems 1–2 are useful only if we have a convenient way to compute the value of $n_k(z')$. When $p > 3$, using the explicit identities (3) it is easy to verify that z' and $-1 - z'$ are the solutions of (10) when $k = 1$. These solutions are distinct if and only if $z' \neq -1/2 \pmod p$. By (4), the condition $z' \neq -1/2 \pmod p$ implies that $F'(z') \neq 0 \pmod p$ when $p > 3$ so that Hensel's lemma (see [7, Ch. I, Th. 3]) implies that for these values of z' and these primes p the congruence in (10) has exactly two solutions for every $k > 1$, too. When $z' = -1/2 \pmod p$ the condition $F'(z') \neq 0 \pmod p$ is violated, Hensel's lemma is not applicable in its simpler form, and more solutions can appear. The following lemma will be used firstly to prove Proposition 3 below providing the exact number of solutions for every $p > 3$, and secondly for the proof of a part of Proposition 4 giving the analogous result in the special case $p = 3$.

LEMMA 1. *Let p be an odd prime. Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a map represented by a power series. Assume that $f'(z_0) = 0$ at a unique p-adic integer z_0, and that $f''(z) \neq 0 \pmod p$ and $f'''(z) = 0 \pmod p$ for every $z \in \mathbb{Z}_p$. Let $z' \in \mathbb{Z}_p$ with $z' = z_0 \pmod p$. Finally, let ν_0 be the p-adic exponent of $z' - z_0$. Then, for every k the number of solutions of*

$$\begin{cases} f(z) = f(z') \pmod{p^k}, \\ z = z_0 \pmod p, \end{cases} \tag{11}$$

is

$$\begin{cases} 2p^{\nu_0} & \text{if } \nu_0 \leq \lfloor (k-1)/2 \rfloor, \\ p^{\lfloor k/2 \rfloor} & \text{if } \nu_0 > \lfloor (k-1)/2 \rfloor. \end{cases}$$

Proof. By hypothesis $\nu_0 > 0$. Since $f''(z) \neq 0 \pmod p$, from $f'(z') = f''(z_0)(z' - z_0) + O(p(z' - z_0))$ we conclude that $p^{\nu_0} \parallel f'(z')$. It is convenient to define $m \in \mathbb{Z}$ in such a way that $f'(z') = mp^{\nu_0} \pmod{p^{\nu_0+1}}$ and to set $\ell := \lfloor (k-1)/2 \rfloor$.

Step 1. The p-adic exponent of $n!$ is $(n-s_n)/(p-1)$, where s_n denotes the sum of the digits of the p-adic representation of n. In particular, it is always strictly lower than $n/2$ for positive n and odd p.

Step 2. Let z be a solution of (11) and let $s \in \mathbb{N}$ be such that $p^s \parallel (z-z')$. We prove that $s \geq \min(\nu_0, \ell+1)$.

Note that $s > 0$, because $\nu_0 > 0$ and $p \mid (z-z_0)$ by hypothesis. Suppose $s < \min(\nu_0, \ell+1)$. Then $2s+1 \leq 2\ell+1 \leq k$, hence we can reduce modulo p^{2s+1} the congruence $f(z) = f(z') \pmod{p^k}$. In this way we obtain

$$0 = f(z) - f(z') = f'(z')(z-z') + \frac{1}{2}f''(z')(z-z')^2 + \frac{1}{6}f'''(z')(z-z')^3 \pmod{p^{2s+1}},$$

since the order in p of each term $(1/n!)f^{(n)}(z')(z-z')^n$ is strictly larger than $ns - n/2$ (by Step 1), which is $\geq 2s$ for $n \geq 4$. Moreover, $p^{\nu_0+s} \parallel f'(z')(z-z')$ and $\nu_0 + s \geq 2s+1$ by hypothesis, hence the first term in the previous congruence is 0 modulo p^{2s+1}; also the last term is zero modulo p^{2s+1} (for $p = 3$ this is true because we are assuming that $f'''(z')$ is divisible by p). In this way from the previous congruence we get

$$0 = (z-z')^2 \pmod{p^{2s+1}},$$

which is a contradiction.

Step 3. We prove that if $\nu_0 > \ell$, then for every z' there are $p^{\lfloor k/2 \rfloor}$ solutions to (11).

Let z be a solution. By Step 2 we know that $z = z' + hp^{\ell+1}$ for some integer h. Moreover, modulo p^k we have

$$f(z' + hp^{\ell+1}) - f(z') = f'(z')hp^{\ell+1}$$

because the terms $(1/n!)f^{(n)}(z')h^n p^{n(\ell+1)}$ are of order strictly larger than $n(\ell+1) - n/2$ (by Step 1), which is $\geq k-1$ for $n \geq 2$. Since $\nu_0 + \ell + 1 \geq 2\ell + 2 \geq k$ we have

$$f(z' + hp^{\ell+1}) - f(z') = f'(z')hp^{\ell+1} = mhp^{\nu_0+\ell+1} = 0$$

for every choice of h. This argument shows that in this case the solutions of (11) are the numbers of the form $z' + hp^{\ell+1}$ with any $h \pmod{p^{k-\ell-1}}$. The claim follows since $p^{k-\ell-1} = p^{\lfloor k/2 \rfloor}$.

Step 4. We prove that if $\nu_0 = \ell$ and k odd, then for every z' there are $2p^\ell$ solutions to (11).

We notice that by assumption $\nu_0 \geq 1$, hence $\ell \geq 1$, so that this step applies only for $k \geq 3$. Let z be a solution. By Step 2 we know that $z = z' + hp^{\nu_0}$ for some h. Moreover, the order of each term $(1/n!)f^{(n)}(z')h^n p^{n\nu_0}$ in p is strictly larger than $n\nu_0 - n/2$ (by Step 1). Since $\nu_0 = (k-1)/2$, the

nth term is at least of order k whenever $n \geq 2(k-1)/(k-2)$, i.e. whenever $n \geq 4$. It follows that modulo p^k we have

$$\begin{aligned} f(z'+hp^{\nu_0}) - f(z') &= f'(z')hp^{\nu_0} + \frac{1}{2}f''(z')h^2p^{2\nu_0} + \frac{1}{3!}f'''(z')h^3p^{3\nu_0} \\ &= \left(mh + \frac{1}{2}f''(z')h^2 + \frac{1}{3!}f'''(z')h^3p^{\nu_0}\right)p^{2\nu_0}. \end{aligned}$$

Since $2\nu_0 = k-1$, the congruence $f(z'+hp^{\nu_0}) = f(z') \pmod{p^k}$ becomes

$$mh + \frac{1}{2}f''(z')h^2 + \frac{1}{3!}f'''(z')h^3p^{\nu_0} = 0 \pmod{p}.$$

Recalling that we are assuming that $f''(z') \neq 0 \pmod{p}$ and $f'''(z') = 0 \pmod{p}$, we can simplify this equation to

$$2mh + f''(z')h^2 = 0 \pmod{p},$$

thus we have two solutions for h modulo p. In this way, we get $2p^{k-(\nu_0+1)} = 2p^{\ell}$ solutions.

Step 5. We prove that if $\nu_0 = \ell$ and k even, then for every z' there are $2p^{\ell}$ solutions to (11).

We notice that by assumption $\nu_0 \geq 1$, hence $\ell \geq 1$, so that this step applies only for $k \geq 4$. Let z be a solution. By Step 2 we know that $z = z' + hp^{\nu_0}$ for some h. Moreover, the order of each term $(1/n!)f^{(n)}(z')h^np^{n\nu_0}$ in p is strictly larger than $n\nu_0 - n/2$ (by Step 1). Since $\nu_0 = (k-2)/2$, the nth term is at least of order k whenever $n \geq 2(k-1)/(k-3)$, i.e. whenever $n \geq 6$. Moreover, every odd prime divides 5! at most once, so that also the term with $n = 5$ is of order at least k. It follows that modulo p^k we have

$$\begin{aligned} f(z'+hp^{\nu_0}) - f(z') &= f'(z')hp^{\nu_0} + \frac{1}{2}f''(z')h^2p^{2\nu_0} \\ &\quad + \frac{1}{6}f'''(z')h^3p^{3\nu_0} + \frac{1}{4!}f^{(4)}(z')h^4p^{4\nu_0}. \end{aligned}$$

Thus

$$\begin{aligned} &f(z'+hp^{\nu_0}) - f(z') \\ &\qquad = mhp^{2\nu_0} + \frac{1}{2}f''(z')h^2p^{2\nu_0} + \frac{1}{6}f'''(z')h^3p^{3\nu_0} + \frac{1}{4!}f^{(4)}(z')h^4p^{4\nu_0}. \end{aligned}$$

Since $2\nu_0 = k-2$, we obtain in this way a solution to $f(z) = f(z') \pmod{p^k}$ whenever

$$mh + \frac{1}{2}f''(z')h^2 + \frac{1}{6}f'''(z')h^3p^{\nu_0} + \frac{1}{4!}f^{(4)}(z')h^4p^{k-2} = 0 \pmod{p^2}. \tag{12}$$

The term $\frac{1}{6}f'''(z')h^3p^{\nu_0}$ is divisible by p because $\nu_0 \geq 1$ (when $p = 3$ we use the assumption $f'''(z') = 0 \pmod{p}$); also $(1/4!)f^{(4)}(z')h^4p^{k-2}$ is divisible by p because $k-2 \geq 2$ and the term 4! in the denominator erases at

most one power of p (and only when $p = 3$). It follows that this equation modulo p becomes $mh + \frac{1}{2}f''(z')h^2 = 0$, having two distinct solutions for h: 0 and $-2m(f''(z'))^{-1}$. Since the value of the derivative (in h) of the function appearing on the L.H.S. in (12) is zero only at $h = -m(f''(z'))^{-1} \pmod p$, we see that each solution of (12) modulo p lifts in a unique way to a solution modulo p^2. Concluding, we have proved that (12) has two solutions; in this way, we get $2p^{k-(\nu_0+2)} = 2p^\ell$ solutions of (11).

Step 6. Steps 3–5 prove the claim whenever $\nu_0 \geq \ell$. Suppose now that $\nu_0 < \ell$ so that $2\nu_0 + 1 < k$. Hensel's lemma (see [14, Ch. 1, Sec. 6.4]) shows that each solution modulo $p^{2\nu_0+1}$ lifts to a unique solution modulo p^k; in this way we see that the number of solutions modulo p^k is equal to the number of solutions modulo $p^{2\nu_0+1}$, i.e. $2p^{\nu_0}$ (by Step 4), which is the claim. ∎

Proposition 3. *Let $p > 3$ be a prime and let ν_0 be such that $p^{\nu_0} \parallel (z' - z_0)$, where z_0 is given in* (4). *Then*

$$n_k(z') = \begin{cases} 2p^{\nu_0} & \text{if } \nu_0 \leq \lfloor (k-1)/2 \rfloor, \\ p^{\lfloor k/2 \rfloor} & \text{if } \nu_0 > \lfloor (k-1)/2 \rfloor. \end{cases}$$

Proof. The discussion before Lemma 1 proves the claim when $\nu_0 = 0$; the claim for $\nu_0 \geq 1$ is an immediate consequence of Lemma 1. ∎

The case $p = 3$ behaves in a different and more complicated way because there are numbers z' and integers k for which the congruence $F(z) = F(z') \pmod{3^k}$ admits more solutions than $F(z) = F(z') \pmod{3^{k+1}}$; for example, there are ten solutions for $F(z) = F(3^2 + 2 \cdot 3^3) \pmod{3^4}$ while the same equation admits only one solution modulo 3^5. In other words, not every solution modulo 3^k can be lifted to a 3-adic solution. The following table shows the solutions of $F(z) = F(z') \pmod 3$ for each z':

z'	Solutions
0	0 (simple), 2 (double)
1	1 (simple)
2	0 (simple), 2 (double)

By Hensel's lemma, each simple solution lifts to a unique solution modulo 3^k for every $k > 1$, so that if $z' = 1 \pmod 3$ there is a unique solution for every k; in other cases more solutions modulo 3^k appear. The next proposition gives the exact number of solutions for every z'. In order to formulate it we need a second constant that, as z_0, has a special role: let z_1 be the 3-adic integer such that $z_1 = 0 \pmod 3$ and $F(z_1) = F(z_0)$. Its existence and uniqueness follow by Hensel's lemma from the congruences $F(0) = F(z_0)$

(mod 3) and $F'(0) = 2 \pmod 3$, and its approximate value is

$$z_1 = 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + 3^5 + 2\cdot 3^6 + 3^7 + 2\cdot 3^8 + 3^{10} + 3^{12} + 2\cdot 3^{13} + 3^{14} + 2\cdot 3^{16} + O(3^{17}).$$

PROPOSITION 4. *Assume $p = 3$ in* (10).

- *If $z' = 0 \pmod 3$ and ν_1 is such that $3^{\nu_1} \parallel (z' - z_1)$, then*

$$n_k(z') = \begin{cases} 1 + 2\cdot 3^{\nu_1/2} & \text{if } \nu_1 \text{ is even, } z' = z_1 + 2\cdot 3^{\nu_1} \pmod{3^{\nu_1+1}}, \\ & \text{and } \nu_1 < k, \\ 1 + 3^{\lfloor k/2\rfloor} & \text{if } \nu_1 \geq k, \\ 1 & \text{otherwise.} \end{cases}$$

- *If $z' = 1 \pmod 3$ then $n_k(z') = 1$ for every k.*
- *If $z' = 2 \pmod 3$ and ν_0 is such that $3^{\nu_0} \parallel (z' - z_0)$, then*

$$n_k(z') = \begin{cases} 1 + 2\cdot 3^{\nu_0} & \text{if } \nu_0 \leq \lfloor (k-1)/2\rfloor, \\ 1 + 3^{\lfloor k/2\rfloor} & \text{if } \nu_0 > \lfloor (k-1)/2\rfloor. \end{cases}$$

Proof. The case $z' = 1 \pmod 3$ has been proved during the discussion preceding Proposition 4, thus we suppose now that $z' = 0$ or $2 \pmod 3$. According to the table above, there is one solution congruent to 0 (mod 3) and this solution lifts uniquely to a solution modulo 3^k for every k, therefore $n_k(z') - 1$ counts the solutions of

$$F(z) = F(z') \pmod{3^k}, \qquad z = 2 \pmod 3. \tag{13}$$

If $z' = 2 \pmod 3$, the number of solutions of (13) is determined by Lemma 1, hence to complete the proof of the theorem we have to consider the case $z' = 0 \pmod 3$.

STEP 1. By definition, ν_1 is the 3-adic exponent of $z' - z_1$ and our assumptions imply that $\nu_1 \geq 1$. We have

$$F(z') - F(z_0) = F(z_1 + (z' - z_1)) - F(z_1) = F'(z_1)(z' - z_1) + O(3(z' - z_1)),$$

proving that $3^{\nu_1} \parallel (F(z') - F(z_0))$.

STEP 2. Suppose that $\nu_1 \geq k$, so that $F(z') = F(z_0) \pmod{3^k}$. Under this assumption the congruence $F(z) = F(z') \pmod{3^k}$ is equivalent to $F(z) = F(z_0) \pmod{3^k}$, which has $3^{\lfloor k/2\rfloor}$ solutions congruent to 2 (mod 3), according to Lemma 1.

STEP 3. We now prove that for every m the solutions of $F(z) = F(z_0) \pmod{3^m}$ with $z = 2 \pmod 3$ are the numbers $\{z_0 + 3^{\lfloor (m+1)/2\rfloor} h\}_{h=1}^{3^{\lfloor m/2\rfloor}}$.

In fact, this set contains $3^{\lfloor m/2\rfloor}$ distinct numbers and in the previous step we have proved that the equation has exactly $3^{\lfloor m/2\rfloor}$ solutions. Moreover we

have the Taylor series

$$F(z_0+3^{\lfloor (m+1)/2\rfloor}h) = F(z_0)+F'(z_0)3^{\lfloor (m+1)/2\rfloor}h+\sum_{n\ge 2}^{\infty}\frac{F^{(n)}(z_0)}{n!}3^{n\lfloor (m+1)/2\rfloor}h^n.$$

The order in 3 of $(F^{(n)}(z_0)/n!)3^{n\lfloor (m+1)/2\rfloor}h^n$ is at least $n\lfloor (m+1)/2\rfloor - (n-s_n)/2$, where s_n denotes the sum of the digits appearing in the 3-adic representation of n. It is easy to prove that $n\lfloor (m+1)/2\rfloor - (n-s_n)/2 \ge m$ for every $m \ge 1$ and every $n \ge 2$, and it follows that the Taylor series gives

$$F(z_0 + 3^{\lfloor (m+1)/2\rfloor}h) = F(z_0) + F'(z_0)3^{\lfloor (m+1)/2\rfloor}h + O(3^m).$$

Since $F'(z_0) = 0$ (by definition of z_0) we conclude that every number of that set is a solution of the congruence.

Step 4. Assume now that $\nu_1 < k$. By Step 1, reducing (13) modulo 3^{ν_1} we obtain the system

$$\begin{cases} F(z) = F(z_0) \pmod{3^{\nu_1}}, \\ z = 2 \pmod 3. \end{cases}$$

According to the previous discussion, z must be equal to $z_0 + 3^{\ell+1}h$ for a suitable integer h, where for convenience we set $\ell := \lfloor (\nu_1 - 1)/2\rfloor$. Taking this into account in (13) and using $F'(z_0) = 0$ and $F''(z_0) = 2 \pmod 3$ we get (modulo 3^k)

$$0 = F(z')-F(z) = F(z')-F(z_0+3^{\ell+1}h) = F(z')-F(z_0)-3^{2\ell+2}h^2+O(3^{2\ell+3})$$

(in order to prove the claim for $\ell = 0$ we use the congruence $F'''(z) = 0 \pmod 3$) so that

$$F(z') - F(z_0) = 3^{2\ell+2}h^2 + O(3^{2\ell+3}) \pmod{3^k}. \tag{14}$$

If ν_1 is odd, then $\ell = (\nu_1 - 1)/2$, the R.H.S. is divisible by 3^{ν_1+1} while the L.H.S. is divisible only by 3^{ν_1}, by Step 1, so in this case we have no solutions.

Now suppose ν_1 even. Then $\ell = \nu_1/2 - 1$ and dividing (14) by 3^{ν_1} we see that

$$\frac{F(z') - F(z_0)}{3^{\nu_1}} = h^2 + O(3). \tag{15}$$

This equation has solutions for h if and only if $(F(z') - F(z_0))/3^{\nu_1} = 1 \pmod 3$, i.e. iff $F(z') = F(z_0) + 3^{\nu_1} + O(3^{\nu_1+1})$, and it is easy to see that this happens iff $z' = z_1 + 2\cdot 3^{\nu_1} + O(3^{\nu_1+1})$. In this way we see that if $\nu_1 < k$ then in order to have solutions it is necessary that

$$\begin{cases} \nu_1 \text{ even}, \\ z' = z_1 + 2 \cdot 3^{\nu_1} + O(3^{\nu_1+1}). \end{cases} \tag{16}$$

Let us assume that these conditions hold true. Suppose that $k = \nu_1+1$. Then h is not subject to any condition except (15); in particular, every number

of the form $z_0 \pm 3^{\nu_1/2} + h'3^{\nu_1/2+1}$ solves (13). When h' assumes the values $1, \dots, 3^{\nu_1/2}$ we get $2 \cdot 3^{\nu_1/2}$ distinct solutions, in agreement with the claim.

Step 5. Suppose that $k > \nu_1 + 1$ and that (16) holds. Reducing modulo 3^{ν_1+1} the congruence $F(z) = F(z') \pmod{3^k}$ we obtain an equation having $2 \cdot 3^{\nu_1/2}$ solutions, all of type $z_0 \pm 3^{\nu_1/2} + h'3^{\nu_1/2+1}$. Let $\tilde{z}$ be an arbitrary number of this form. This number solves $F(z) = F(z') \pmod{3^{\nu_1+1}}$, moreover

$$\begin{aligned} F'(\tilde{z}) &= F'(z_0 \pm 3^{\nu_1/2} + \tilde{h}3^{\nu_1/2+1}) = F'(z_0) \pm F''(z_0)3^{\nu_1/2} + O(3^{\nu_1/2+1}) \\ &= \mp 3^{\nu_1/2} + O(3^{\nu_1/2+1}) \end{aligned}$$

(because $F'(z_0) = 0$ and $F''(z_0) = 2 \pmod 3$), which shows that $3^{\nu_1/2} \parallel F'(\tilde{z})$. Hence the 3-adic exponent of $F'(\tilde{z})$ is strictly lower than $(\nu_1 + 1)/2$. Hensel's lemma (as given in [14, Ch. 1, Sec. 6.4]) proves that under these conditions $\tilde{z}$ can be lifted in a unique way to a solution of $F(z) = F(z')$ in $\mathbb{Z}_3$. In particular, the equation modulo 3^k has as many solutions congruent to 2 modulo 3 as the same equation modulo 3^{ν_1+1}, i.e. $2 \cdot 3^{\nu_1/2}$. ∎

Using Theorem 1 and Propositions 3–4 we can compute the number of distinct Gauss sums and distinct signatures that we have modulo p^k, when p is an odd prime and $k > 1$.

Theorem 3. *For every $k > 1$ and $p \geq 3$ the number of distinct Gauss sums and the number of distinct signatures modulo p^k are $\Psi(p^k)\Phi(p-1)$ and $\Psi(p^k)\Phi^*(p-1)$, respectively.*

Proof. Each character χ is uniquely determined by its χ_U and χ_V components. Every couple (u, z') with $u \in U_k$ and $z' \in \mathbb{Z}_{p^{k-1}}$ uniquely determines χ_V but leaves χ_U undetermined, hence there are $p-1$ characters χ with $u_\chi = u$ and $z_\chi = z'$ (because we can choose χ_U in $p-1$ ways). For every d dividing $p-1$ there are $\varphi(d)$ numbers u in U_k of order d (because U_k is cyclic), hence for every choice of z' there are $(p-1)\varphi(d)$ characters χ with $z_\chi = z'$ and u_χ of order d. By Theorem 1 each value of the Gauss sum for a character in this set is assumed $(p-1)n_{k-2}(z')/d$ times, hence the number of distinct Gauss sums which are associated to characters in this set is

$$\frac{(p-1)\varphi(d)}{(p-1)n_{k-2}(z')/d} = \frac{d\varphi(d)}{n_{k-2}(z')}.$$

For every integer r, let $m(r)$ denote the number of distinct z' for which $n_{k-2}(z') = r$. The previous argument shows that for every given integer $d \,|\, (p-1)$ and every r there are

$$\frac{m(r)}{r}\, d\varphi(d)$$

distinct Gauss sums. Since $m(r)$ is independent of d we find that the number

of distinct Gauss sums is

$$\sum_r \sum_{d|p-1} \frac{m(r)}{r} d\varphi(d) = \sum_r \frac{m(r)}{r} \Phi(p-1).$$

In order to complete the proof of the first formula we need an explicit evaluation of the sum over r. When $k = 2$ we have $m(1) = 1$ and $m(r) = 0$ for every $r > 1$, thus the formula is proved in this case. Let now $k > 2$. The cases $p = 3$ and $p > 3$ split, due to the different structure of Propositions 3 and 4.

Suppose $p > 3$. By Proposition 3 we know that $m(r) \neq 0$ only when r is either of the form $2p^\nu$ or $p^{\lfloor k/2 \rfloor - 1}$ (recall that we are considering $n_{k-2}(z')$ while Proposition 3 provides $n_k(z')$, hence the normalization $k \to k-2$ is needed). Moreover, for every $\nu \leq \lfloor (k-3)/2 \rfloor$ we have $n_{k-2}(z') = 2p^\nu$ iff $p^\nu \parallel (z' - z_0)$. Since z' is taken modulo p^{k-2}, there are $\varphi(p^{k-\nu-2})$ possible values for z' satisfying $p^\nu \parallel (z' - z_0)$. On the other hand, we have $n_{k-2}(z') = p^{\lfloor k/2 \rfloor - 1}$ iff $p^{\lfloor (k-3)/2 \rfloor + 1} | (z' - z_0)$; modulo p^{k-2} there are $p^{k - \lfloor (k-3)/2 \rfloor - 3}$ values of z' satisfying this condition. Summarizing, we have

$$\begin{aligned} \sum_r \frac{m(r)}{r} &= \sum_{\nu=0}^{\lfloor (k-3)/2 \rfloor} \frac{\varphi(p^{k-\nu-2})}{2p^\nu} + \frac{p^{k-\lfloor (k-3)/2 \rfloor - 3}}{p^{\lfloor k/2 \rfloor - 1}} \\ &= 1 + \frac{p-1}{2} \sum_{\nu=0}^{\lfloor (k-3)/2 \rfloor} p^{k-2\nu-3} = 1 + \frac{p^{k-1} - p^\delta}{2(p+1)} \end{aligned}$$

where $\delta \in \{0, 1\}$ with $\delta + k = 1 \pmod 2$. By definition, this is $\Psi(p^k)$, thus the proof of the first claim is complete in this case.

Suppose $p = 3$. By Proposition 4 we know that $m(r) \neq 0$ only when r is either 1, or of the form $1 + 2 \cdot 3^\nu$ or $1 + 3^{\lfloor k/2 \rfloor - 1}$ (as before, recall that we are considering $n_{k-2}(z')$ while Proposition 4 provides $n_k(z')$, hence the normalization $k \to k-2$ is needed).

According to Proposition 4 we have $n_{k-2}(z') = 1$ in three cases:

(1) $z' = 1 \pmod 3$,
(2) $z' = z_1 \pm 3^\nu + O(3^{\nu+1})$, with $\nu < k-2$ and odd,
(3) $z' = z_1 + 3^\nu + O(3^{\nu+1})$, ν even and $1 < \nu < k-2$.

Therefore

$$m(1) = 3^{k-3} + \sum_{\substack{\nu \in [1, k-2) \\ \nu \text{ odd}}} 2 \cdot 3^{k-3-\nu} + \sum_{\substack{\nu \in [1, k-2) \\ \nu \text{ even}}} 3^{k-3-\nu}.$$

Writing this sum as $3^{k-3} + \sum_{\nu=1}^{k-3} \frac{3-(-1)^\nu}{2} 3^{k-3-\nu}$ we get, after some computations,

$$m(1) = \frac{5 \cdot 3^{k-2} - 6 + (-1)^k}{8}.$$

We have $n_{k-2}(z') = 1+3^{\lfloor k/2\rfloor -1}$ when either $z = z' \pmod{3^{k-2}}$ or $3^{\lfloor (k-3)/2\rfloor +1} \mid (z'-z_0)$, i.e. in $3^{k-\lfloor (k-3)/2\rfloor -3}$ cases. Hence $m(1+3^{\lfloor k/2\rfloor -1}) = 1+3^{k-\lfloor (k-3)/2\rfloor -3}$.

Finally, for every $\nu \le \lfloor (k-3)/2\rfloor$ we have $n_{k-2}(z') = 1 + 2\cdot 3^{\nu}$ when either $z' = z_1 + 2\cdot 3^{2\nu} + O(3^{2\nu+1})$, or $z' = z_0 \pm 3^{\nu} + O(3^{\nu+1})$. In the first case we have $3^{k-2-(2\nu+1)}$ choices for z' and in the second case there are $2\cdot 3^{k-2-(\nu+1)}$ choices, so that $m(1+2\cdot 3^{\nu}) = 3^{k-2\nu-3} + 2\cdot 3^{k-\nu-3}$.

Summarizing, we have

$$\begin{aligned}\sum_r \frac{m(r)}{r} &= \frac{5\cdot 3^{k-2} - 6 + (-1)^k}{8} + \frac{1+3^{k-3-\lfloor (k-3)/2\rfloor}}{1+3^{\lfloor k/2\rfloor -1}} \\ &\quad + \sum_{\nu=1}^{\lfloor (k-3)/2\rfloor} \frac{3^{k-2\nu-3}(1+2\cdot 3^{\nu})}{1+2\cdot 3^{\nu}} \\ &= \frac{5\cdot 3^{k-2} - 6 + (-1)^k}{8} + 1 + \frac{3^{k-1} - 3^{\delta}}{8} - 3^{k-3}\end{aligned}$$

where $\delta \in \{0,1\}$ with $\delta + k = 1 \pmod 2$. With trivial simplifications we see that this sum is simply $2\cdot 3^{k-3}$, which is exactly the value of $\Psi(3^k)$. The proof of the first claim is now complete.

The claim about signatures can be proved in a similar way. ∎

Theorem 3 can be generalized in the following way. As usual, let $q = p^k$ with $p \ge 3$ and $k > 1$. Let $G^{(0)}$ be the set of values τ of Gauss sums of primitive characters modulo q for which $-\tau$ is not the value of a Gauss sum, let $G^{(+)}$ be a set of representatives under the action of ± 1 of the values which are not in $G^{(0)}$, and finally let $G^{(-)}$ be the complementary set (the negatives of the values in $G^{(+)}$, hence). By Theorem 2 the values in $G^{(0)}$ are those values of Gauss sums which are associated with characters χ whose parameter d_χ is odd, while the values in $G^{(\pm)}$ are those associated with characters χ whose parameter d_χ is even. An argument similar to that giving Theorem 3 yields the following result.

THEOREM 4. *Write p as $1 + 2^N m$ with m odd. Then*

$$|G^{(0)}| = \Psi(p^k)\Phi(m),$$

$$|G^{(\pm)}| = \frac{1}{2}\Psi(p^k)(\Phi(p-1) - \Phi(m)) = \frac{\Phi(2^N)-1}{2}\Psi(p^k)\Phi(m).$$

The next subsections illustrate some non-trivial consequences of the previous theorems. Mainly we will show that the cases $q = p^2$ and $q = p^3$ are in some sense exceptional, because for these prime powers there are still characters modulo q with $|W(\chi)| = 1$, i.e. characters χ for which $L(s,\chi)$ is the unique solution (with Euler product) of the corresponding functional equation. Moreover, we will show that this phenomenon disappears when $q = p^k$ with $k \ge 4$ because for these powers $|W(\chi)|$ is always greater than 2.

Moreover, we shall see that the value of $|W(\chi)|$ is two for more than half the signatures, and that only occasionally does it reach its largest value which is of order $\sqrt{q}$.

The following fact is a first, and quite unexpected, consequence of Theorem 3: for every p^k the quotient "number of distinct signatures/number of distinct Gauss sums" depends on p but is independent of k; in fact

$$\frac{|\{\text{distinct signatures mod } p^k\}|}{|\{\text{distinct Gauss sums mod } p^k\}|} = \frac{\Phi^*(p-1)}{\Phi(p-1)} = 1 + \frac{1}{\Phi(2^N)} = 1 + \frac{3}{2^{2N+1}+1} \tag{17}$$

where we have set $p = 1 + 2^N m$ for a suitable odd integer m, and where we have used (2) to simplify the quotient $\Phi^*(p-1)/\Phi(p-1)$. It is immediate to see that the universal bound

$$\frac{|\{\text{distinct signatures mod } p^k\}|}{|\{\text{distinct Gauss sums mod } p^k\}|} \le 1 + \frac{1}{3}$$

holds with equality for primes $p = 3 \pmod 4$ (giving $N = 1$ in (17)), and that

$$\liminf_{p\to\infty} \frac{|\{\text{distinct signatures mod } p^k\}|}{|\{\text{distinct Gauss sums mod } p^k\}|} = 1,$$

because for every integer N there are infinitely many primes $p = 1 \pmod{2^N}$.

3.1. Consequences: modulo p^2. Each character χ is uniquely determined by its components χ_U and χ_V, and χ_V is in its turn uniquely determined by the couple (u_χ, z_χ). For every d dividing $p-1$ there are $\varphi(d)$ numbers $u \in U_k$ of order d; moreover, 0 is the unique value available for z_χ when $q = p^2$, so that $n_0(z_\chi) = 1$. It follows that for every d there are $\varphi(d)\cdot 1$ possible choices for χ_V. Since there are $p-1$ possible choices for χ_U, we conclude that there are $(p-1)\varphi(d)$ characters χ for which u_χ has order d. By Theorem 1 the values of the Gauss sums of characters in this set are assumed $(p-1)/d$ times, hence there are exactly $d\varphi(d)$ distinct values for the Gauss sums which are assumed $(p-1)/d$ times. In particular, there are $(p-1)\varphi(p-1)$ Gauss sums whose values are assumed only once.

In a similar way we can prove that for every d dividing $p-1$, among the $(p-1)\varphi(d)$ characters χ with $d_\chi = d$ there are exactly $d^*\varphi(d)$ distinct signatures whose values are assumed $(p-1)/d^*$ times. Hence a signature is assumed only once iff $d^* = p-1$. When $p = 1 \pmod 4$ the unique possibility is $d = p-1$ so that there are $d^*\varphi(d) = (p-1)\varphi(p-1)$ such signatures ($p-1$ is even, hence $(p-1)^* = p-1$). When $p = 3 \pmod 4$ we have $d^* = p-1$ both for $d = p-1$ and for $d = (p-1)/2$, hence in this case there are $(p-1)\varphi(p-1) + (p-1)\varphi((p-1)/2)$ such signatures.

Since $\varphi((p-1)/2) = \varphi(p-1)$ when $p = 3 \pmod 4$, we have proved that the number of signatures which are assumed only once is

$$2^\natural(p-1)\varphi(p-1) \quad \text{where} \quad 2^\natural := \begin{cases} 1 & \text{if } p = 1 \pmod 4, \\ 2 & \text{if } p = 3 \pmod 4. \end{cases}$$

3.2. Consequences: modulo p^3. Also in this case the number of primitive characters whose Gauss sum is assumed only once and the number of primitive characters whose signature is assumed only once are

$$(p-1)\varphi(p-1) \quad \text{and} \quad 2^\natural(p-1)\varphi(p-1)$$

respectively. In fact, by Theorem 1 the Gauss sum is assumed only once iff $n_1(z_\chi) = 1$ and $d_\chi = p-1$, while the signature is assumed only once iff $n_1(z_\chi) = 1$ and $d_\chi^* = p-1$. Since $n_1(z')$ is 1 only for $z' = (p-1)/2$ (by Proposition 3 if $p > 3$ and by Proposition 4 if $p = 3$), the claim follows as in the proof of the previous claim for p^2.

A similar argument shows that there are $\frac{p-1}{2}\big(\varphi\big(\frac{p-1}{2}\big) + (p-1)\varphi(p-1)\big)$ values of Gauss sums each assumed twice and that the number of signatures which are assumed twice is:

$$\begin{cases} \frac{p-1}{2}\big[(p-1)\varphi(p-1) + \varphi\big(\frac{p-1}{2}\big)\big] & \text{if } p = 1 \pmod 8, \\ (p-1)^2\varphi(p-1) & \text{if } p = 3 \pmod 4, \\ \frac{p-1}{2}\big[(p-1)\varphi(p-1) + \varphi\big(\frac{p-1}{2}\big) + \varphi\big(\frac{p-1}{4}\big)\big] & \text{if } p = 5 \pmod 8. \end{cases}$$

3.3. Consequences: modulo p^k with $k \geq 4$. Proposition 3 shows that $n_{k-2}(z_\chi) \geq 2$ when $k \geq 4$ and $p > 3$. By Theorem 1 we conclude that in this case the value of each Gauss sum and each signature is assumed at least twice. Actually, the number of Gauss sum values and the number of signatures which are assumed exactly twice are

$$\frac{1}{2}(p-1)^2p^{k-3}\varphi(p-1) \quad \text{and} \quad \frac{2^\natural}{2}(p-1)^2p^{k-3}\varphi(p-1),$$

respectively. In fact, by Theorem 1 the value of a Gauss sum is assumed twice iff $d = p-1$ (hence $\varphi(p-1)$ choices for u_χ) and $n_{k-2}(z') = 2$. By Proposition 3 we have $n_{k-2}(z') = 2$ iff $z' \neq (p-1)/2 \pmod p$, so that we have $p^{k-2} - p^{k-3}$ possible values for z', producing $\varphi(p-1)(p^{k-2} - p^{k-3})$ choices for χ_V. As usual we have $p-1$ choices for χ_U, so that we have exactly $(p-1)\varphi(p-1)(p^{k-2} - p^{k-3})$ characters χ whose Gauss sum has a value which is assumed twice. Dividing this number by 2 we obtain the number of values of Gauss sums which are assumed twice.

Analogously, by Theorem 1 a signature is assumed twice iff $d^* = p-1$ and $n_{k-2}(z') = 2$, thus we have $p^{k-2} - p^{k-3}$ possible values for z', as before. Moreover, when $p = 1 \pmod 4$ we have $d^* = p-1$ only for $d = p-1$, while for $p = 3 \pmod 4$ we have $d^* = p-1$ both for $d = p-1$ and for $d = (p-1)/2$. Thus in the first case the number of signatures is equal to

the number of values of Gauss sums already computed, while in the second case it is twice that number.

Suppose $p = 3$. Proposition 4 shows that 2 is not the minimum value for $n_{k-2}(z_\chi)$, since $n_{k-2}(z') = 1$ for several values of z'. Indeed, in the proof of Theorem 3 we have shown that $n_{k-2}(z') = 1$ for $(5 \cdot 3^{k-2} - 6 + (-1)^k)/8$ choices of z', and using this formula we can prove that the number of Gauss sums and of signatures which are assumed only once are

$$\frac{5 \cdot 3^{k-2} - 6 + (-1)^k}{4} \quad \text{and} \quad \frac{5 \cdot 3^{k-2} - 6 + (-1)^k}{2}$$

respectively. In fact, by Theorem 1 the value of the Gauss sum of χ is assumed once iff $d_\chi = 2$ and $n_{k-2}(z_\chi) = 1$; since there is a unique $u \in U_k$ having order 2, $(5 \cdot 3^{k-2} - 6 + (-1)^k)/8$ is also the number of couples (u, z') meeting those requirements. Since every couple uniquely determines the component χ_V of the character χ, we see that $(5 \cdot 3^{k-2} - 6 + (-1)^k)/8$ is the number of possible choices for χ_V. There are two choices for χ_U, hence the first formula immediately follows. The formula for signatures can be proved in a similar way by noticing that by Theorem 1 a signature is assumed once iff $d^* = 2$ and $n_{k-2}(z') = 1$ and that $d^*_\chi = 2$ for every character.

For $p > 3$, let

$$\mathcal{G}_{p,k} := \frac{|\text{values of Gauss sums mod } p^k \text{ assumed twice}|}{|\text{values of Gauss sums mod } p^k|},$$

$$\mathcal{S}_{p,k} := \frac{|\text{signatures mod } p^k \text{ assumed twice}|}{|\text{signatures mod } p^k|},$$

and analogously for $p = 3$ let

$$\mathcal{G}_{3,k} := \frac{|\text{values of Gauss sums mod } 3^k \text{ assumed once}|}{|\text{values of Gauss sums mod } 3^k|},$$

$$\mathcal{S}_{3,k} := \frac{|\text{signatures mod } 3^k \text{ assumed once}|}{|\text{signatures mod } 3^k|}.$$

The previous formulæ and Theorem 3 show that

$$\mathcal{G}_{p,\infty} := \lim_{k\to\infty} \mathcal{G}_{p,k} = \begin{cases} \dfrac{p^2-1}{p^2} \cdot \dfrac{(p-1)\varphi(p-1)}{\Phi(p-1)} & \text{if } p > 3, \\ 5/8 & \text{if } p = 3, \end{cases}$$

and

$$\mathcal{S}_{p,\infty} := \lim_{k\to\infty} \mathcal{S}_{p,k} = \begin{cases} \dfrac{p^2-1}{p^2} \cdot \dfrac{2^{\natural}(p-1)\varphi(p-1)}{\Phi^*(p-1)} & \text{if } p > 3, \\ 15/16 & \text{if } p = 3. \end{cases}$$

These limits show that a positive (and large) proportion of the values of Gauss sums and signatures are assumed only the smallest number of times. We now prove explicit bounds for these proportions.

PROPOSITION 5. *For $p > 3$ we have*

$$\alpha \cdot \frac{p^2-1}{p^2} \le \mathcal{G}_{p,\infty} \le \frac{3}{4},$$

$$\alpha \cdot \frac{p^2-1}{p^2} \le \mathcal{S}_{p,\infty} \le \frac{3}{4} \quad \text{if } p = 1 \pmod 4,$$

$$\frac{3}{2}\,\alpha \cdot \frac{p^2-1}{p^2} \le \mathcal{S}_{p,\infty} \le \frac{8}{9} \quad \text{if } p = 3 \pmod 4,$$

with $\alpha := \prod_r \left(1 - \frac{1+r}{1+r^3}\right) = 0.5145\ldots$, where the product is over all primes.

Proof. By multiplicativity we have, for every integer n,

$$\frac{n\varphi(n)}{\Phi(n)} = \prod_{r^j \| n} \left(1 - \frac{1+r^{2j-1}}{1+r^{2j+1}}\right),$$

where r runs over all primes. Each factor increases with j, therefore we have

$$\prod_r \left(1 - \frac{1+r}{1+r^3}\right) \le \prod_{r|n} \left(1 - \frac{1+r}{1+r^3}\right) \le \frac{n\varphi(n)}{\Phi(n)} \le \prod_{r|n} \left(1 - \frac{1}{r^2}\right) \le \frac{3}{4}.$$

Moreover, writing $n = 2^N m$ with m odd, we have

$$\frac{n\varphi(n)}{\Phi^*(n)} = \frac{2^N\varphi(2^N)}{1+\Phi(2^N)} \cdot \frac{m\varphi(m)}{\Phi(m)} = \frac{3\cdot 2^{2N-1}}{4+2^{2N+1}} \cdot \prod_{r^j \| m} \left(1 - \frac{1+r^{2j-1}}{1+r^{2j+1}}\right).$$

Let now $p = 1 + 2^N m$ with m odd. For primes $p = 1 \pmod 4$ we have (in this case $N > 1$ but m can be equal to 1)

$$\frac{2}{3} \cdot \prod_{r|m} \left(1 - \frac{1+r}{1+r^3}\right) \le \frac{3\cdot 2^{2N-1}}{4+2^{2N+1}} \cdot \prod_{r|m} \left(1 - \frac{1+r}{1+r^3}\right) \le \frac{2^\natural(p-1)\varphi(p-1)}{\Phi^*(p-1)}$$

$$= \frac{3\cdot 2^{2N-1}}{4+2^{2N+1}} \cdot \prod_{r^j \| m} \left(1 - \frac{1+r^{2j-1}}{1+r^{2j+1}}\right) \le \frac{3}{4} \cdot \prod_{r|m} \left(1 - \frac{1}{r^2}\right) \le \frac{3}{4},$$

while for primes $p = 3 \pmod 4$ we have (in this case $N = 1$ and $m \ge 3$)

$$\prod_{r>2} \left(1 - \frac{1+r}{1+r^3}\right) \le \prod_{r|m} \left(1 - \frac{1+r}{1+r^3}\right)$$

$$\le \frac{2^\natural(p-1)\varphi(p-1)}{\Phi^*(p-1)} = \prod_{r^j \| m} \left(1 - \frac{1+r^{2j-1}}{1+r^{2j+1}}\right) \le \prod_{r|m} \left(1 - \frac{1}{r^2}\right) \le \frac{8}{9}.$$

These computations prove the claim. ∎

Each bound appearing in Proposition 5 is optimal. For example, for every $n \in \mathbb{N}$ let w_n be a prime such that $w_n = 1 + P_n \pmod{P_n^2}$, where $P_n := \prod_{j=1}^{n} p_j$ and $\{p_j\}_j$ is the sequence of all primes. The existence of such a prime is ensured by Dirichlet's theorem on primes in arithmetic progressions, since $1 + P_n$ and P_n^2 are evidently coprime. Then $w_n - 1 = P_n(1 + P_n k_n)$ for some integer k_n so that

$$\frac{(w_n-1)\varphi(w_n-1)}{\Phi(w_n-1)} = \prod_{j\le n}\left(1-\frac{1+p_j}{1+p_j^3}\right)\prod_{r^j\|(1+P_nk_n)}\left(1-\frac{1+r^{2j-1}}{1+r^{2j+1}}\right).$$

When n grows to infinity the first factor tends to α and the second to 1, because each factor of $1 + P_n k_n$ is greater than p_n, so that

$$1 > \prod_{r^j\|(1+P_nk_n)}\left(1-\frac{1+r^{2j-1}}{1+r^{2j+1}}\right) > \prod_{r^j\|(1+P_nk_n)}\left(1-\frac{2}{r^2}\right) \ge \prod_{d>p_n}\left(1-\frac{2}{d^2}\right)$$

and the R.H.S. tends to 1 as n grows; this argument proves that $\lim_{n\to\infty} \mathcal{G}_{w_n,\infty} = \alpha$. In a similar way, let w_n be a prime such that $w_n = 1 + 2^{n\varphi(P'_n)} \pmod{2^n P'_n}$ where $P'_n := \prod_{j=2}^{n} p_j$ is the product over the sequence of odd primes. As before the existence of such a prime is ensured by Dirichlet's theorem, since $1 + 2^{n\varphi(P'_n)}$ and $2^n P'_n$ are coprime (because $1 + 2^{n\varphi(P'_n)}$ is odd and for every odd prime p_j dividing P'_n we have $1 + 2^{n\varphi(P'_n)} = 2 \pmod{p_j}$). Then $w_n - 1 = 2^{h_n}(2^{n\varphi(P'_n)-h_n} + P'_n k_n)$ where h_n is the greatest power of 2 dividing $w_n - 1$, so that

$$\frac{(w_n-1)\varphi(w_n-1)}{\Phi(w_n-1)} = \left(1-\frac{1+2^{2h_n-1}}{1+2^{2h_n+1}}\right)\prod_{r^j\|(2^{n\varphi(P'_n)-h_n}+P'_nk_n)}\left(1-\frac{1+r^{2j-1}}{1+r^{2j+1}}\right).$$

When n grows to infinity the first factor tends to $3/4$ (because $h_n \ge n$) and the second to 1, therefore $\lim_{n\to\infty} \mathcal{G}_{w_n,\infty} = 3/4$. With a similar approach it is possible to determine suitable sequences of primes proving the optimality of the bounds for $\mathcal{S}_{p,\infty}$.

4. Composite conductors. For the moment let q be still an odd prime power, but let us consider the general equation $\tau(\chi, \zeta_q) = \vartheta\tau(\psi, \zeta_q)$. To what extent the presence of the generic qth root of unity ζ_q affects the set of solutions of this equation? It is not difficult to answer this question since the cyclotomic field $\mathbb{Q}[e(1/\varphi(q)), \zeta_q] = \mathbb{Q}[e(1/(p-1)), \zeta_q]$ has an automorphism σ such that $\sigma(\zeta_q) = e(1/q)$ (the automorphism is uniquely determined if we also require that $\sigma(e(1/(p-1))) = e(1/(p-1))$), so that

$$\tau(\chi,\zeta_q) = \vartheta\tau(\psi,\zeta_q) \;\Leftrightarrow\; \sigma(\tau(\chi,\zeta_q)) = \vartheta\sigma(\tau(\psi,\zeta_q)) \;\Leftrightarrow\; \tau(\chi_\zeta) = \vartheta\tau(\psi_\zeta)$$

where $\chi_\zeta := \sigma \circ \chi$ and $\psi_\zeta := \sigma \circ \psi$ are new primitive Dirichlet characters. Therefore, the characters ψ solving the equation can be recovered by

applying the methods of the previous sections to χ_ζ and composing the solutions with σ^{-1}. We can also be a bit more explicit. Let $b_\zeta \in \mathbb{Z}_q^*$ be such that $\zeta_q = e(b_\zeta^{-1}/q)$, where b_ζ^{-1} denotes the inverse of b_ζ in $\mathbb{Z}_q^*$. Then $\sigma(\chi(1+p)) = \sigma(e(-a_\chi p/q)) = e(-a_\chi b_\zeta p/q)$, proving that $a_{\chi_\zeta} = b_\zeta a_\chi$. In particular, if we decompose b_ζ as $u_\zeta(1+z_\zeta p)$ with $u_\zeta \in U_k$ and $1+z_\zeta p \in V_k$, we find that $u_{\chi_\zeta} = u_\zeta u_\chi$ and $z_{\chi_\zeta} = z_\chi + z_\zeta + z_\chi z_\zeta p$. By Proposition 2 we conclude that $\tau(\psi, \zeta_q) = \vartheta\tau(\chi, \zeta_q)$ iff

$$\begin{cases} u_\chi = u_\psi, \\ \chi(u_\zeta u_\chi) = \vartheta\psi(u_\zeta u_\psi), \\ F(z_\chi + z_\zeta + z_\chi z_\zeta p) = F(z_\psi + z_\zeta + z_\psi z_\zeta p) \pmod{p^{k-2}}. \end{cases}$$

These relations show in a concrete way how the equality is influenced by the root ζ_q: the number of solutions is still given by Theorem 1, with d_χ replaced by the order of $u_\zeta u_\chi$, and z_χ by $z_\chi + z_\zeta + z_\chi z_\zeta p$.

Let now q be a composite number, $q = q'p^k$ with q', p odd integers and p prime, $p \nmid q'$. Let χ be a primitive character modulo q and let χ', χ_p be the primitive characters modulo q' and p^k, respectively, such that $\chi = \chi'\chi_p$. Let ζ_q be a primitive qth root of unity and let $\zeta_{q'}$ and ζ_{p^k} be primitive roots of unity such that $\tau(\chi, \zeta_q) = \tau(\chi', \zeta_{q'})\tau(\chi_p, \zeta_{p^k})$. Let ψ be another primitive character modulo q, with components ψ' and ψ_p, and suppose that $\tau(\chi, \zeta_q) = \vartheta\tau(\psi, \zeta_q)$; then

$$\frac{\tau(\psi', \zeta_{q'})}{\tau(\chi', \zeta_{q'})} = \vartheta \frac{\tau(\chi_p, \zeta_{p^k})}{\tau(\psi_p, \zeta_{p^k})}. \tag{18}$$

In this equality, the L.H.S. is in $\mathbb{Q}[e(1/\varphi(q')), \zeta_{q'}]$ while the R.H.S. is in $\mathbb{Q}[e(1/\varphi(p^k)), \zeta_{p^k}]$. If we assume that $(q'\varphi(q'), p\varphi(p)) = 2$, then those cyclotomic fields intersect only in $\mathbb{Q}$ and from (18) we deduce that

$$\frac{\tau(\psi', \zeta_{q'})}{\tau(\chi', \zeta_{q'})} = \vartheta', \quad \frac{\tau(\chi_p, \zeta_{p^k})}{\tau(\psi_p, \zeta_{p^k})} = \vartheta_p \tag{19}$$

where $\vartheta', \vartheta_p \in \{\pm 1\}$ and $\vartheta'\vartheta_p = \vartheta$. By induction on the number of distinct primes dividing q we obtain from (19) the following result.

THEOREM 5. *Let $q = \prod_{j=1}^n p_j^{k_j}$ be the decomposition of q into distinct prime powers. Let χ be a primitive character modulo q, for every j let χ_j be the primitive character modulo $p_j^{k_j}$ such that $\chi = \prod_{j=1}^n \chi_j$ and let ζ_j be the $p_j^{k_j}$th primitive root of unity such that $\tau(\chi) = \prod_{j=1}^n \tau(\chi_j, \zeta_j)$. Let ψ be another primitive character modulo q and let ψ_j for $j = 1, \dots, n$ be its component at $p_j^{k_j}$. If $(p_j(p_j-1), p_l(p_l-1)) = 2$ for every $j \neq l$, then $\tau(\chi) = \tau(\psi)$ iff there exists $\boldsymbol{\vartheta} = (\vartheta_1, \dots, \vartheta_n) \in \{\pm 1\}^n$ with $\vartheta_1 \cdots \vartheta_n = 1$ such that $\tau(\chi_j, \zeta_j) = \vartheta_j \tau(\psi_j, \zeta_j)$ for every j.*

Note that by Proposition 1 we know that $\chi_j = \psi_j$ and $\vartheta_j = 1$ is the unique solution of $\tau(\chi_j, \zeta_j) = \vartheta_j \tau(\psi_j, \zeta_j)$ when $k_j = 1$, hence it is sufficient to consider the squarefull case. Collecting the previous results and using the multiplicativity as suggested by the previous theorem we now prove upper and lower bounds for $|T(\chi)|$ and $|W(\chi)|$ for composite q satisfying the hypothesis in Theorem 5.

THEOREM 6. *Suppose* $q = \prod_{j=1}^{n} p_j^{k_j}$ *with* $(p_j(p_j-1), p_l(p_l-1)) = 2$ *for* $j \neq l$, $k_j \geq 2$ *and* $n \geq 2$. *Then*

$$|T(\chi)| \leq \frac{3^{n+1/2}}{\sqrt{q'}}\sqrt{q}, \tag{20}$$

where q' *is the product of primes dividing* q *with odd order, i.e.* $q' := \prod_{j=1}^{n} p_j^{\delta_j}$ *with* $\delta_j \in \{0,1\}$ *and* $\delta_j = k_j \pmod 2$. *This bound is essentially optimal because there exists an effective constant* $c > 0$ *such that for every* q *satisfying the hypothesis there exists a primitive character* χ_q *modulo* q *for which*

$$|W(\chi_q)| \geq \frac{c}{\sqrt{q'}}\sqrt{q}. \tag{21}$$

Proof. Upper bound (20). For every factor $p_j^{k_j}$ the number of characters ψ_j with $\tau(\chi_j, \zeta_j) = \tau(\psi_j, \zeta_j)$ is bounded by $2(p_j-1)p_j^{k_j/2-\delta_j/2-1}$ (by Th. 1 and Prop. 3) when $p_j > 3$, and by $2(p_j-1)p_j^{k_j/2-1}$ (by Th. 1 and Prop. 4) when $p_j = 3$. Analogously, the number of characters ψ_j with $\tau(\chi_j, \zeta_j) = -\tau(\psi_j, \zeta_j)$ is bounded by $2\frac{p_j-1}{2}p_j^{k_j/2-\delta_j/2-1}$ (by Th. 2 and Prop. 3) when $p_j > 3$, and by $2\frac{p_j-1}{2}p_j^{k_j/2-1}$ (by Th. 2 and Prop. 4) when $p_j = 3$. It follows that the number of characters ψ_j with $\tau(\chi_j, \zeta_j) = \pm\tau(\psi_j, \zeta_j)$ is bounded by $3p_j^{k_j/2-\delta_j/2}$ when $p_j > 3$, and by $3p_j^{k_j/2}$ when $p_j = 3$. By Theorem 5 we conclude that $|T(\chi)| \leq 3^n\sqrt{3q/q'}$ by multiplicativity.

Lower bound (21). For every j we fix a character χ_j modulo $p_j^{k_j}$ with z_{χ_j} such that $n_{k_j-2}(z_{\chi_j}) \geq p_j^{\lfloor k_j/2 \rfloor - 1}$ and $d_{\chi_j} = 2$ for $j = 1, \ldots, n-1$, while $d_{\chi_n} = 1$. Let χ be the character modulo q whose component at $p_j^{k_j}$ is χ_j, for every j. For every j, let $T_{j,+}$ be the set of characters ψ_j such that $\tau(\psi_j) = \tau(\chi_j)$, and $T_{j,-}$ the set of ψ_j such that $\tau(\psi_j) = -\tau(\chi_j)$. By Theorems 1–2 there are at least $\frac{p_j-1}{2}p_j^{\lfloor k_j/2 \rfloor - 1}$ characters in $T_{j,+}$ and $\frac{p_j-1}{2}p_j^{\lfloor k_j/2 \rfloor - 1}$ characters in $T_{j,-}$, when $j = 1, \ldots, n-1$.

We now fix ψ_j in $T_{j,+} \cup T_{j,-}$ for $j = 1, \ldots, n-2$ and ψ_{n-1} in either $T_{n-1,+}$ or $T_{n-1,-}$ in such a way that $\vartheta_1 \cdots \vartheta_{n-1} = 1$. We notice that these choices can be done in $\frac{1}{2}\prod_{j=1}^{n-1}(p_j-1)p_j^{\lfloor k_j/2 \rfloor - 1}$ ways. Finally, we take ψ_n in such a way that $\tau(\chi_n) = \tau(\psi_n)$ and with parity such that $\psi_n(-1) \cdot \prod_{j=1}^{n-1}\psi_j(-1) =$

$\chi(-1)$; we can make this choice in $\frac{p_n-1}{2}p_n^{\lfloor k_n/2\rfloor-1}$ different ways because by Theorem 1 there are $(p_n-1)p_n^{\lfloor k_n/2\rfloor-1}$ characters whose Gauss sum is $\tau(\chi_n)$ and only $\frac{p_n-1}{2}p_n^{\lfloor k_n/2\rfloor-1}$ characters having also the same parity (because we are assuming $d_{\chi_n}=1$). The character $\psi := \psi_1\cdots\psi_n$ satisfies both $\psi(-1) = \chi(-1)$ and $\tau(\chi, e(1/p_1^{k_1}+\cdots+1/p_n^{k_n})) = \tau(\psi, e(1/p_1^{k_1}+\cdots+1/p_n^{k_n}))$, and our construction shows that there are at least

$$\frac{1}{4}\prod_{j=1}^{n}(p_j-1)p_j^{\lfloor k_j/2\rfloor-1} = \frac{1}{4}\prod_{j=1}^{n}\left(1-\frac{1}{p_j}\right)\frac{\sqrt{q}}{\sqrt{q'}} \tag{22}$$

such characters. A suitable automorphism converts that equality to an equality of Gauss sums at the principal qth root, therefore (21) will follow from (22) after we prove the existence of a universal positive lower bound for the product $\prod_{j=1}^{n}(1-p_j^{-1})$, or, what is the same, of the existence of a universal upper bound for $\sum_{j=1}^{n}p_j^{-1}$, when the primes satisfy the assumption of this theorem.

Let Θ denote any set of odd primes $\{p_j\}_{j=1}^{n}$ for which $(p_j(p_j-1), p_l(p_l-1)) = 2$ for $j\neq l$. For every k let $S'_k := |\Theta\cap(2^k,2^{k+1}]|$ and let $S(2^k,\Theta) := |\{m\in(2^k,2^{k+1}] : m\neq 0,1 \pmod p\ \forall p\in\Theta\cap(1,2^k)\}|$. Note that $S'_k\le S(2^k,\Theta)$, by the hypothesis on the primes. A standard result in sieve theory (see [11, Th. 3.13]) gives the bound

$$S(2^k,\Theta)\ll\frac{2^k}{k^2}\prod_{p\in\Theta\cap(1,2^k)}\left(1-\frac{2}{p}\right)\left(1-\frac{1}{p}\right)^{-2}\le\frac{2^k}{k^2}.$$

It follows that $S'_k\ll 2^k/k^2$, uniformly in Θ, and the claim immediately follows. ∎

Remark. The previous result involves a severe restriction on possible values for q; we believe that a result of the form

$$|T(\chi)|\ll_\epsilon q^{1/2+\epsilon},\qquad |W(\chi)| = \Omega_\epsilon(q^{1/2-\epsilon})$$

for every $\epsilon>0$, should hold for every q.

Finally, we give a formula for the number of distinct values assumed by the Gauss sum and by the signature modulo integers q satisfying the hypothesis of Theorem 5. That hypothesis implies that only at most one prime congruent to 1 modulo 4 divides q. It is possible to produce a formula for the number of distinct Gauss sums modulo q even when such a prime exists, but the result is simpler when all primes dividing q are congruent to 3 modulo 4. The following theorem gives the formulæ for this simpler case.

Theorem 7. *Let $q=\prod_{j=1}^{n}p_j^{k_j}$ with $k_j\ge 2$ and $p_j = 3 \pmod 4$ for every j. Suppose that $(p_j(p_j-1), p_l(p_l-1)) = 2$ for every $j\neq l$. Finally,*

for every j let $m_j := (p_j - 1)/2$. Then the number of distinct Gauss sums modulo q is

$$(2^{n+1} - 1)\Psi(q)\Phi\Big(\prod_{j=1}^{n} m_j\Big),$$

and the number of distinct signatures modulo q is

$$4(2^n - 1)\Psi(q)\Phi\Big(\prod_{j=1}^{n} m_j\Big).$$

Proof. For every j we partition the set of Gauss sums modulo $p_j^{k_j}$ into three classes: $G_j^{(0)}$, $G_j^{(-)}$ and $G_j^{(+)}$, as in Theorem 4. Note that $|G_j^{(0)}| = |G_j^{(\pm)}| = \Psi(p_j^{k_j})\Phi(m_j)$, because we are assuming that $p_j = 3 \pmod 4$. Let $\tau(\chi)$ be a Gauss sum modulo q. We decompose it as product $\prod_{j=1}^{n} \tau(\chi_j, \zeta_j)$ that for convenience of notation we write as $\prod_{j=1}^{n} \tau_j$. We associate with τ a string of n symbols $s_1, \dots, s_n$ taken in $\{0, -1, +1\}$, by setting $s_j = 0$, -1, or $+1$ whenever τ_j belongs to $G_j^{(0)}$, $G_j^{(-)}$ or $G_j^{(+)}$, resp. Let two strings $\mathbf{s}, \mathbf{s}'$ associated with the Gauss sums of two characters be given; if there exists $\bar{\jmath}$ such that $s_{\bar{\jmath}} = 0$ and $s'_{\bar{\jmath}} = \pm 1$ (or vice versa) then the Gauss sums are distinct. In fact, for the equality of these Gauss sums by Theorem 5 we must have $\tau_{\bar{\jmath}} = \vartheta_{\bar{\jmath}} \tau'_{\bar{\jmath}}$ with $\vartheta_{\bar{\jmath}} \in \{\pm 1\}$; the case $\vartheta_{\bar{\jmath}} = 1$ is impossible, since by hypothesis $\tau_{\bar{\jmath}}$ and $\tau'_{\bar{\jmath}}$ belong to distinct $G_{\bar{\jmath}}$ sets. Also the case $\vartheta_{\bar{\jmath}} = -1$ is impossible, since the equality $\tau_{\bar{\jmath}} = -\tau'_{\bar{\jmath}}$ would imply $\tau_{\bar{\jmath}} \in G_{\bar{\jmath}}^{(-)} \cup G_{\bar{\jmath}}^{(+)}$, contrary to assumption.

Moreover, if in a string $\mathbf{s}$ we invert two non-zero symbols (hence $-1 \leftrightarrow +1$) we obtain a new string $\mathbf{s}'$ corresponding to a Gauss sum with the same value, by Theorem 5 again; as a consequence, the following list provides a set of representative and mutually inequivalent strings that are therefore associated with distinct Gauss sums:

$$\begin{aligned}
&\{\text{the string } (0, \dots, 0)\} \\
&\quad \cup \{\text{strings with } h \text{ symbols } 0, \text{ and } +1 \text{ in the other positions}\}_{h=0}^{n-1} \\
&\quad \cup \{\text{strings with } h \text{ symbols } 0, \text{ the symbol } -1 \text{ in the first free position,} \\
&\qquad \text{and } +1 \text{ in the other positions}\}_{h=0}^{n-1}.
\end{aligned}$$

This list contains $1 + 2\sum_{h=0}^{n-1} \binom{n}{h} = 2^{n+1} - 1$ strings. Each string, independently of its content on symbols $-1, 0$ and $+1$, produces $\prod_{j=1}^{n} \Psi(p_j^{k_j})\Phi(m_j)$ distinct Gauss sums and the claim follows.

We have already noted that the parameter d_{χ_j} of characters χ_j with Gauss sums in $G_j^{(\pm)}$ is even; these characters have equal Gauss sums if

and only if they have equal signatures. On the other hand, the parameter d_{χ_j} of characters χ_j with Gauss sums in $G_j^{(0)}$ is odd; the Gauss sums of these characters are assumed both by characters with the same parity and by characters with the opposite parity. It follows that when we count the number of signatures modulo q adopting the same procedure we used for Gauss sums, each string containing at least one 0 contributes twice, while the strings without 0 contribute only once. The total number of contributions is therefore $2\big(1+2\sum_{h=1}^{n-1}\binom{n}{h}\big)+2 = 4(2^n-1)$ times the number of contributions of each term, which is $\prod_{j=1}^{n}\Psi(p_j^{k_j})\Phi(m_j)$, as before. ∎

Acknowledgements. The author warmly thanks the anonymous referee for his valuable comments and suggestions which have considerably improved the general presentation of this paper.

This material is partially based upon work supported by the National Science Foundation under agreement No. DMS-0635607.

References

[1] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, Canad. Math. Soc. Ser. Monogr. Adv. Texts, Wiley, New York, 1998.

[2] S. Bochner, *On Riemann's functional equation with multiple Gamma factors*, Ann. of Math. (2) 67 (1958), 29–41.

[3] T. Funakura, *A generalization of the Chowla–Mordell theorem on Gaussian sums*, Bull. London Math. Soc. 24 (1992), 424–430.

[4] P. Gérardin and W. Li, *Functional equations and periodic sequences*, in: Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, 267–279.

[5] J. Kaczorowski, G. Molteni, and A. Perelli, *A converse theorem for Dirichlet L-functions*, Comment. Math. Helv. 85 (2010), 463–483.

[6] J. Kaczorowski and A. Perelli, *On the structure of the Selberg class. I.* $0 \le d \le 1$, Acta Math. 182 (1999), 207–241.

[7] N. Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions*, 2nd ed., Springer, New York, 1984.

[8] J.-L. Mauclaire, *Sommes de Gauss modulo* p^α. *I*, Proc. Japan Acad. Ser. A Math. Sci. 59 (1983), no. 3, 109–112.

[9] —, *Sommes de Gauss modulo* p^α. *II*, ibid. 59 (1983), no. 4, 161–163.

[10] G. Molteni, *Multiplicity results for the functional equation of the Dirichlet L-functions: case* $p = 2$, Acta Arith. 145 (2010), 71–81.

[11] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory. I. Classical Theory*, Cambridge Stud. Adv. Math. 97, Cambridge Univ. Press, Cambridge, 2007.

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

[13] I. Piatetski-Shapiro and R. Raghunathan, *On Hamburger's theorem*, in: Lie Groups and Lie Algebras: E. B. Dynkin's Seminar, Amer. Math. Soc. Transl. (2) 169, Amer. Math. Soc., Providence, RI, 1995, 109–120.

[14] A. M. Robert, *A Course in p-Adic Analysis*, Grad. Texts in Math. 198, Springer, New York, 2000.
[15] M.-F. Vignéras, *Facteurs gamma et équations fonctionnelles*, in: Modular Functions of One Variable, VI (Bonn, 1976), Lecture Notes in Math. 627, Springer, Berlin, 1977, 79–103.

G. Molteni
Dipartimento di Matematica
Università di Milano
via Saldini 50
I-20133 Milano, Italy
E-mail: giuseppe.molteni1@unimi.it

Received on 21.10.2009
and in revised form on 9.2.2010 (6182)