ACTA ARITHMETICA
145.1 (2010)

Multiplicity results for the functional equation of the Dirichlet L-functions: case $p = 2$

by

G. Molteni (Milano)

1. Introduction. For any given primitive character χ modulo q, the set $W(\chi)$ has been introduced in [3]; roughly speaking, it is the set of Dirichlet series $F(s)$ absolutely converging for $\sigma > 1$, having a representation as Euler product for $\sigma > 1$ and meromorphic continuation to $\mathbb{C}$ with a unique possible pole at $s = 1$, and satisfying the functional equation

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

where $a(\chi) := (1-\chi(-1))/2$ is the parity of χ and $\tau(\chi)$ is its Gauss sum. The dependence of the functional equation on the character χ is completely described by the *signature* of χ, i.e. by the couple of numbers $s(\chi) := (\chi(-1), \tau(\chi))$, and notwithstanding its axiomatic definition, it is known that the only members of $W(\chi)$ are the Dirichlet L-functions associated with characters having the same signature of χ. For this reason (but with abuse of notation) we identify $W(\chi)$ with the set $\{\psi : s(\psi) = s(\chi)\}$. In [3] it has been proved that $W(\chi)$ reduces to the unique function $L(s,\chi)$ (pursuing with the abuse, we write that $W(\chi) = \{\chi\}$ in this case) for every χ modulo q essentially only for squarefree q (but some repeated factors are allowed at primes 2 and 3). In [6] we have generalized this result by giving explicit formulæ and optimal upper/lower bounds for the cardinalities of the set $W(\chi)$, of the set $T(\chi) := \{\psi : \tau(\psi) = \tau(\chi)\}$ and of the set of distinct signatures and of distinct Gauss sums, when q is either an odd prime power or a composite squarefull number with prime factors of a special form. The case $q = 2^k$ was not included in that analysis, as a consequence of the peculiar

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

DOI: 10.4064/aa145-1-4

structure of the group $\mathbb{Z}_{2^k}^*$. The present paper fills this gap, reproducing for the prime 2 the analysis we have already done for the other prime powers. In particular, we prove two results. The first one gives the cardinalities of $T(\chi)$ and $W(\chi)$ in terms of the parameters $n_k(z_\chi)$ and u_χ which are described in the next sections.

THEOREM 1. *Let χ be a primitive character modulo 2^k with $k \geq 5$. Then*
$$|T(\chi)| = \begin{cases} n_{k-2}(z_\chi)/2 & \text{if } u_\chi = 1, \\ n_{k-3}(z_\chi)/2 & \text{if } u_\chi = -1, \end{cases} \quad \text{and} \quad |W(\chi)| = n_{k-2}(z_\chi)/4.$$

The second result gives the cardinalities of the images of the maps τ and s.

THEOREM 2. *Let $k \geq 5$. The number of distinct Gauss sums and the number of distinct signatures modulo 2^k are respectively*
$$\frac{2^{k-2} + 27 - (-1)^k}{6} \quad \text{and} \quad \frac{2^{k-2} + 18 + 2(-1)^k}{3}.$$

In view of the previous discussion, the second part of Theorem 1 counts the solutions of the functional equation (1), and the second part of Theorem 2 counts the number of functional equations of type (1) with a conductor $q = 2^k$. When coupled to Proposition 2 of Section 3 giving a simple algorithm for the computation of $n_k(z_\chi)$, these theorems immediately imply the following facts:

(1) There exists a primitive character χ modulo 2^k with $|W(\chi)| = 1$ iff $k \leq 6$. In other words, when $k > 6$ the functional equation (1) always has at least two distinct solutions.
(2) $|W(\chi)| \leq 2^{\lfloor k/2 \rfloor - 2}$ when $k \geq 6$.
(3) If $k \geq 9$, then $|W(\chi)| = 2$ iff z_χ is odd. Thus $|W(\chi)| = 2$ for exactly half primitive characters and
$$\lim_{k \to \infty} \frac{|\{\text{signatures mod } 2^k \text{ assumed twice}\}|}{|\{\text{signatures mod } 2^k\}|} = \frac{3}{4}.$$
In other words, for $k > 9$ there is 50% chance for a random primitive character modulo 2^k to produce a functional equation (1) with exactly two solutions, and 75% chance for a random functional equation (1) to have exactly two solutions.
(4) When $k \geq 6$ and k is even (odd, resp.) there are exactly four (sixteen, resp.) distinct signatures which are assumed $2^{\lfloor k/2 \rfloor - 2}$ times.

From the qualitative point of view, these facts agree with the general behavior of $W(\chi)$ for conductors of the type we have considered in [6].

The paper is organized as follows: in Section 2 we recall some well known facts to fix our notation and we give the definitions of some new objects; in Section 3 we prove Theorems 1 and 2.

2. Preliminary facts

2.1. Gauss sums. Given an integer q, a character χ modulo q, and a primitive qth root of unity ζ_q, the Gauss sum is defined as $\tau(\chi,\zeta_q) := \sum_{n=1}^{q}\chi(n)\zeta_q^n$. For convenience, we denote by $\tau(\chi)$ the Gauss sum $\tau(\chi, e(1/q))$. Explicit formulæ for Gauss sums when q is a squarefull prime power have been found by Odoni [7] for odd primes, and extended to the prime 2 by Funakura [2]; an alternative proof has been given by Mauclaire [4, 5] (see also [1]).

2.2. Group $\mathbb{Z}^*_{2^k}$. When $q = 2^k$ with $k \geq 3$, the multiplicative group $\mathbb{Z}^*_q$ can be decomposed as the direct product of the subgroups U_k and V_k, which are the cyclic groups generated by -1 and by 5, respectively. This decomposition gives an analogous decomposition of each character χ modulo q as $\chi_U\chi_V$, where χ_U is a character of U_k and χ_V is a character of V_k. With respect to this decomposition, χ is even iff χ_U is trivial, and χ is primitive iff $\chi_V(5)$ is a primitive 2^{k-2}th root of unity. Let χ be primitive; we denote by a_χ the odd integer such that $\chi(5) = e(4a_\chi/q)$; this integer is unique modulo 2^{k-2}. Suppose $k \geq 5$. Then we can decompose a_χ as $u_\chi v_\chi$ with $u_\chi \in U_{k-2}$ and $v_\chi \in V_{k-2}$, and we denote by ρ_χ the integer (unique modulo 2^{k-4}) such that $v_\chi = 5^{\rho_\chi}$ in V_{k-2}. Under the same hypothesis about k we can introduce a further integer z_χ by $v_\chi =: 1 + 4z_\chi$; it is unique modulo 2^{k-4}.

Let $\mathbb{Z}_2$ denote the set of dyadic integers. The function $\log(1 + 4z)/\log 5$ is well defined as a bijective map $\mathbb{Z}_2 \to \mathbb{Z}_2$ and ρ_χ coincides modulo 2^{k-4} with the value of this function at z_χ. Finally, χ is uniquely determined by the triplet $(\chi(-1), u_\chi, z_\chi)$, with χ_V in its turn uniquely determined by the couple (u_χ, z_χ) via the identity $\chi(5) = e(4u_\chi(1 + 4z_\chi)/2^k)$. Vice versa, for each triplet $(\mathcal{P}, u, z)$ with $\mathcal{P}$ and u in $\{\pm 1\}$ and $z \pmod{2^{k-4}}$, there exists a primitive character χ such that $(\chi(-1), u_\chi, z_\chi) = (\mathcal{P}, u, z)$.

2.3. A special 2-adic function. Let $C_2 \in \mathbb{Z}_2$ be the dyadic integer defined by

$$C_2 := \frac{-4}{\log 5}(1 - \log(-4/\log 5)) = 1 + 2^9 + 2^{10} + 2^{11} + 2^{13} + O(2^{14})$$

and let $\digamma : \mathbb{Z}_2 \to \mathbb{Z}_2$ be defined by

$$\digamma(z) := (1 + 4z)\frac{\log(1 + 4z)}{\log 5} + zC_2.$$

We notice that

$$\digamma(z) = 6z^2 \pmod{2^3}.$$

Moreover,

$$\digamma'(z) = \frac{4}{\log 5}[\log(1 + 4z) + \log(-4/\log 5)],$$

and an elementary computation proves that $F'(z)=0$ at the unique point

$$z_0 := -\frac{4+\log 5}{16} = 2^3+2^4+2^7+O(2^8).$$

Finally, for every $n\geq 2$ we have

$$\frac{F^{(n)}(z)}{(n-2)!} = \frac{-4}{\log 5}\,\frac{(-4)^{n-1}}{(1+4z)^{n-1}},$$

proving that $2^{2n-2}\parallel F^{(n)}(z)/(n-2)!$ for every $n\geq 2$ and every z in $\mathbb{Z}_2$.

2.4. Notation. Speaking about functional equations it is customary to call the number $a(\chi) := (1-\chi(-1))/2$ the *parity of* χ, while within the theory of characters this name denotes the number $\chi(-1)$ alone. These quantities are evidently related but it is the second one which appears more frequently in this paper: we denote by $\mathcal{P}_\chi$ the parity of χ according to the second definition. Moreover, we recall that we identify $W(\chi)$ with the set $\{\psi : s(\chi)=s(\psi)\}$, and that $T(\chi)$ denotes the set $\{\psi : \tau(\chi)=\tau(\psi)\}$. Finally, we say that an integer ν is the *order* of a 2-adic integer z when ν is the 2-adic exponent of z, i.e. when $2^\nu \parallel z$ in $\mathbb{Z}_2$.

3. Theorems. Let χ be a primitive character modulo 2^k, $k\geq 5$. Funakura [2] proved the following formula for the Gauss sum of χ:

$$\frac{\tau(\chi)}{\sqrt{2^k}} = \varepsilon_\chi\chi(a_\chi)e(a_\chi C_2/2^k)e(a_\chi/8),$$

where $\varepsilon_\chi := (-1)^{(a_\chi^2-1)k/8}$. Using this formula we prove the following fact.

PROPOSITION 1. *Let χ and ψ be primitive characters modulo 2^k with $k\geq 5$. Then*

$$(2)\qquad \tau(\chi)=\tau(\psi) \quad \textit{iff} \quad \begin{cases} \text{(2.a) } u_\chi = u_\psi =: u, \\ \text{(2.b) } F(z_\chi) = F(z_\psi) + \delta 2^{k-3} \pmod{2^{k-2}}, \end{cases}$$

where $\delta = 0$ if $\chi(u)=\psi(u)$, and $\delta=1$ otherwise.

Proof. Suppose that $\tau(\chi)=\tau(\psi)$. Funakura's formula allows us to write this equality as

$$\varepsilon_\chi\chi(a_\chi)e(a_\chi C_2/2^k)e(a_\chi/8) = \varepsilon_\psi\psi(a_\psi)e(a_\psi C_2/2^k)e(a_\psi/8).$$

By raising this equality to the 2^{k-2}th power and recalling that we are assuming $k\geq 5$, we deduce that $e(a_\chi/4)=e(a_\psi/4)$. This equality proves that $a_\chi = a_\psi \pmod 4$ so that $u_\chi = u_\psi =: u$, which is (2.a). Under this hypothesis we get $\varepsilon_\chi = \varepsilon_\psi(-1)^{k(z_\chi - z_\psi)}$ and the equality becomes

$$(-1)^{kz_\chi}\chi(uv_\chi)e(uv_\chi C_2/2^k)e(uv_\chi/8) = (-1)^{kz_\psi}\psi(uv_\psi)e(uv_\psi C_2/2^k)e(uv_\psi/8),$$

i.e.

$$(-1)^{kz_\chi}\chi(u)e(4uv_\chi\rho_\chi/2^k)e(uv_\chi C_2/2^k)e(uv_\chi/8) \\ = (-1)^{kz_\psi}\psi(u)e(4uv_\psi\rho_\psi/2^k)e(uv_\psi C_2/2^k)e(uv_\psi/8).$$

Since $\chi(u), \psi(u) \in \{\pm 1\}$, we can write this equality as

$$4uv_\chi\rho_\chi + uv_\chi C_2 + uv_\chi 2^{k-3} + kz_\chi 2^{k-1} \\ = 4uv_\psi\rho_\psi + uv_\psi C_2 + uv_\psi 2^{k-3} + \delta 2^{k-1} + kz_\psi 2^{k-1} \pmod{2^k}$$

where $\delta = 0$ if $\chi(u) = \psi(u)$, and $\delta = 1$ otherwise. Since $u^2 = 1$ in $\mathbb{Z}_q^*$, we deduce that

$$4v_\chi\rho_\chi + v_\chi C_2 + v_\chi 2^{k-3} + ukz_\chi 2^{k-1} \\ = 4v_\psi\rho_\psi + v_\psi C_2 + v_\psi 2^{k-3} + u\delta 2^{k-1} + ukz_\psi 2^{k-1} \pmod{2^k}.$$

In terms of the parameters z_χ and z_ψ this congruence can be written as

$$(3)\quad \mathcal{F}(z_\chi)+(1+uk)z_\chi 2^{k-3} = \mathcal{F}(z_\psi)+(1+uk)z_\psi 2^{k-3}+u\delta 2^{k-3} \pmod{2^{k-2}}.$$

We are assuming that $k \ge 5$, thus by reducing (3) modulo 2^2 we obtain $\mathcal{F}(z_\chi) = \mathcal{F}(z_\psi) \pmod{2^2}$, implying that the integers z_χ and z_ψ have the same parity (because $\mathcal{F}(z) = 6z^2 \pmod 8$). Hence the previous equation simplifies to

$$\mathcal{F}(z_\chi) = \mathcal{F}(z_\psi) + u\delta 2^{k-3} \pmod{2^{k-2}},$$

which is (2.b), because u is odd. Each step in the previous argument can be reversed, so that under conditions (2.a)–(2.b) we have $\tau(\chi) = \tau(\psi)$. ■

Due to the form of condition (2.b), it is evident that the equations $\mathcal{F}(z) = \mathcal{F}(z') \pmod{2^k}$ and $\mathcal{F}(z) = \mathcal{F}(z') + 2^{k-1} \pmod{2^k}$ are important for our purposes. The following propositions give simple formulæ for the cardinalities of the sets of their solutions.

PROPOSITION 2. *Let $n_k(z')$ be the number of solutions modulo 2^k of the congruence*

$$\mathcal{F}(z) = \mathcal{F}(z') \pmod{2^k}.$$

Then, for every $k > 0$ we have

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

where ν_0 is the order of $z' - z_0$.

Proof. We recall that the 2-adic exponent of $n!$ is $n - s_n$, where s_n denotes the sum of the digits of the binary representation of n. For clarity we split the proof into several steps.

STEP 1. We prove that $2^{\nu_0+2} \parallel \mathcal{F}'(z')$.

Indeed, in $\mathbb{Z}_2$ we have the power series representation

$$F'(z') = F''(z_0)(z'-z_0) + \sum_{n\geq 3} \frac{F^{(n)}(z_0)}{(n-1)!}(z'-z_0)^{n-1}$$

(recall that $F'(z_0)=0$, by definition of z_0). The order of $F''(z_0)(z'-z_0)$ is $2+\nu_0$. For $n\geq 2$ we know that $2^{2n-2} \parallel F^{(n)}(z_0)/(n-2)!$, hence the order of the nth term in the series is $2n-2-\sigma_{n-1}+(n-1)\nu_0$, where σ_{n-1} is the order of $n-1$. This order is strictly larger than $2+\nu_0$ when $n\geq 3$, because a direct inspection shows that the equivalent inequality $(n-2)(2+\nu_0) > \sigma_{n-1}$ is true when $n\geq 3$. It follows that the order of $F'(z')$ is that of $F''(z_0)(z'-z_0)$.

Step 2. Let μ be the order of $z-z'$. We consider the power series representation

$$F(z)-F(z') = \sum_{n\geq 1} \frac{F^{(n)}(z')}{n!}(z-z')^n =: \sum_{n\geq 1} T_n.$$

Step 1 has proved that T_1 has order $2+\nu_0+\mu$, while a direct check shows that the orders of T_2 and T_3 are $1+2\mu$ and $3(1+\mu)$, respectively. Moreover, for $n\geq 3$ the order of $F^{(n)}(z')$ is at least $2(n-1)$, thus each T_n with $n\geq 3$ has order at least $2(n-1)-(n-s_n)+n\mu = n(1+\mu)+s_n-2$. In particular:

(a) for each μ, the order of T_n with $n>2$ is strictly larger than that of T_2, since

$$n(1+\mu)+s_n-2 > 1+2\mu \;\Leftrightarrow\; n+(n-2)\mu+s_n > 3,$$

which is satisfied because $n\geq 3$ and $s_n\geq 1$;

(b) if $\mu>0$ then the order of T_n with $n>3$ is strictly larger than that of T_3, since

$$n(1+\mu)+s_n-2 > 3(1+\mu) \;\Leftrightarrow\; (n-3)(1+\mu)+s_n > 2,$$

which is satisfied because $(n-3)(1+\mu)\geq 2$ and $s_n\geq 1$.

Step 3. Comparing the orders of T_1 and T_2 we have:

(a) If $2+\mu+\nu_0 < 1+2\mu$, i.e. if $\mu > 1+\nu_0$, then the order of $F(z)-F(z')$ is $2+\mu+\nu_0$ and we get a solution of the congruence modulo 2^k iff $\mu\geq k-2-\nu_0$. Thus, every integer of the form $z=z'+h2^\mu$ with $\mu\geq \max\{2+\nu_0, k-2-\nu_0\}$ is a solution. The number of solutions of this type is $2^{k-\max\{2+\nu_0,k-2-\nu_0\}} = 2^{\min\{k-2-\nu_0,2+\nu_0\}}$.

(b) If $2+\mu+\nu_0 > 1+2\mu$, i.e. if $\mu < 1+\nu_0$, then the order of $F(z)-F(z')$ is $1+2\mu$ and we have a solution of the congruence modulo 2^k iff $1+2\mu\geq k$, i.e. iff $\mu\geq (k-1)/2$. It follows that we have solutions of the type we are considering here iff $\nu_0\geq (k-1)/2$. Actually, under this condition every integer of the form $z=z'+h2^\mu$ with $(k-1)/2\leq \mu\leq \nu_0$ modulo 2^k is a solution. As a consequence, the number of solutions of this type is

$\frac{1}{2}\sum_{(k-1)/2\le\mu\le\nu_0} 2^{k-\mu} = 2^{\lfloor (k+1)/2\rfloor} - 2^{k-1-\nu_0}$ (the factor 1/2 appears because for every μ only odd values for h should be considered).

(c) If $2+\mu+\nu_0 = 1+2\mu$, i.e. if $\mu = 1+\nu_0$, then both T_1 and T_2 have order $3+2\nu_0$, while the order of T_3 is $3(2+\nu_0)$ and that of each other T_n is greater (by Step 2(b)). Thus, three ranges for k must be considered:

(i) $k \ge 7+3\nu_0$. In this case we can reduce modulo $2^{7+3\nu_0}$ the original congruence modulo 2^k, obtaining

$$F'(z')2^{1+\nu_0}h + \frac{F''(z')}{2}2^{2+2\nu_0}h^2 + \frac{F'''(z')}{6}2^{3+3\nu_0}h^3 \\ = F(z) - F(z') = 0 \pmod{2^{7+3\nu_0}}$$

where for convenience we have set $z = z' + 2^{1+\nu_0}h$. Recalling the orders of each term, we write the congruence as

$$\frac{F'(z')}{2^{2+\nu_0}}2^{3+2\nu_0}h + \frac{F''(z')}{2^2}2^{3+2\nu_0}h^2 + \frac{F'''(z')}{3\cdot 2^4}2^{6+3\nu_0}h^3 = 0 \pmod{2^{7+3\nu_0}},$$

which becomes

$$\frac{F'(z')}{2^{2+\nu_0}} + \frac{F''(z')}{2^2}h + \frac{F'''(z')}{2^4}2^{3+\nu_0} = 0 \pmod{2^{4+\nu_0}},$$

because h is an odd integer, whose solution is

$$h = h_0 := -\frac{\frac{F'(z')}{2^{2+\nu_0}} + \frac{F'''(z')}{2^4}2^{3+\nu_0}}{\frac{F''(z')}{2^2}} \pmod{2^{4+\nu_0}}.$$

Thus, modulo $2^{7+3\nu_0}$ we have $2^{2+\nu_0}$ solutions of the form $z = z' + 2^{1+\nu_0}(h_0 + h'2^{4+\nu_0}) = z' + h_0 2^{1+\nu_0} + h'2^{5+2\nu_0}$, corresponding to the different choices for h' modulo $2^{2+\nu_0}$. Every such solution lifts in a unique way to a solution in $\mathbb{Z}_2$ by Hensel's lemma (as given in [8, Ch. 1, Sec. 6.4]) because the order of the derivative $F'(z')$ is $2+\nu_0$, which is strictly lower than $(7+3\nu_0)/2$.

(ii) $3+2\nu_0 < k \le 6+3\nu_0$. In this case the congruence modulo 2^k becomes

$$F'(z')2^{1+\nu_0}h + \frac{F''(z')}{2}2^{2+2\nu_0}h^2 = F(z) - F(z') = 0 \pmod{2^k},$$

i.e.

$$\frac{F'(z')}{2^{2+\nu_0}}2^{3+2\nu_0}h + \frac{F''(z')}{2^2}2^{3+2\nu_0}h^2 = 0 \pmod{2^k},$$

giving

$$\frac{F'(z')}{2^{2+\nu_0}} + \frac{F''(z')}{2^2}h = 0 \pmod{2^{k-3-2\nu_0}},$$

whose solution is

$$h = -\frac{\frac{F'(z')}{2^{2+\nu_0}}}{\frac{F''(z')}{2^2}} =: h_0 \pmod{2^{k-3-2\nu_0}}.$$

We obtain $2^{2+\nu_0}$ distinct solutions modulo 2^k by taking

$$z = z' + (h_0 + h' 2^{k-3-2\nu_0}) 2^{1+\nu_0} = z' + h_0 2^{1+\nu_0} + h' 2^{k-2-\nu_0}$$

with arbitrary h' modulo $2^{2+\nu_0}$.

(iii) $k \le 3 + 2\nu_0$. Then every z of the form $z = z' + 2^{1+\nu_0} h$ with h an odd integer is a solution of the congruence $F(z) - F(z') = 0 \pmod{2^k}$ so that there are $2^{k-2-\nu_0}$ solutions of this type.

Step 4. We complete the proof by collecting the results of the previous steps. Suppose $\nu_0 \ge \lfloor k/2 \rfloor - 1$. Then we have $2^{k-2-\nu_0}$ solutions of type in Step 3(a), $2^{\lfloor (k+1)/2 \rfloor} - 2^{k-1-\nu_0}$ solutions of type in Step 3(b) and $2^{k-2-\nu_0}$ of type in Step 3(c)(iii), giving a total of $2^{\lfloor (k+1)/2 \rfloor}$ solutions. Suppose $\nu_0 < \lfloor k/2 \rfloor - 1$, so that $k \ge 4 + 2\nu_0$. Then we have $2^{2+\nu_0}$ solutions of type in Step 3(a), no solution of type in Step 3(b) and $2^{2+\nu_0}$ solutions of type in Step 3(c) (which subcase (i) or (ii) does not matter because both cases produce $2^{2+\nu_0}$ solutions), giving a total of $2^{3+\nu_0}$ solutions. ∎

Proposition 3. *Let $n'_k(z')$ be the number of solutions modulo 2^k of the congruence*

$$F(z) = F(z') + 2^{k-1} \pmod{2^k}. \tag{4}$$

Then for every $k \ge 1$ we have

$$n'_k(z') = 2n_{k-1}(z') - n_k(z') = \begin{cases} k \text{ even}: & \begin{cases} 2^{3+\nu_0} & \text{if } \nu_0 < k/2 - 2, \\ 3 \cdot 2^{k/2} & \text{if } \nu_0 = k/2 - 2, \\ 2^{k/2} & \text{if } \nu_0 \ge k/2 - 1, \end{cases} \\ k \text{ odd}: & \begin{cases} 2^{3+\nu_0} & \text{if } \nu_0 < (k-1)/2 - 1, \\ 0 & \text{if } \nu_0 \ge (k-1)/2 - 1. \end{cases} \end{cases}$$

Proof. By reduction modulo 2^{k-1}, every solution z to (4) produces a solution of $F(z) = F(z') \pmod{2^{k-1}}$, hence it is of the form $z'' + h2^{k-1}$ with z'' taken among the $n_{k-1}(z')$ solutions of $F(z) = F(z') \pmod{2^{k-1}}$ and $h \in \{0, 1\}$. In order to find a solution to (4) we have to exclude from this set of numbers (whose cardinality is $2n_{k-1}(z')$) those satisfying $F(z) = F(z') \pmod{2^k}$ (whose cardinality is $n_k(z')$). ∎

We are now able to prove our main results.

Proof of Theorem 1. Formula for $|T(\chi)|$. We know that two characters χ and ψ have the same Gauss sum iff they satisfy the system

$$\begin{cases} u_\chi = u_\psi, \\ F(z_\chi) = F(z_\psi) + \delta 2^{k-3} \pmod{2^{k-2}}. \end{cases} \tag{5}$$

Suppose that $u_\chi = 1$. Then $\delta = 0$ because $\psi(u_\psi) = 1 = \chi(u_\chi)$ by the first equation, thus the number of distinct z_ψ satisfying the system is $n_{k-2}(z_\chi)$.

The couple (u_ψ, z_ψ) uniquely defines the component ψ_V of ψ, because $\psi(5) = e(4u_\psi(1+4z_\psi)/2^k)$. This identity also shows that z_ψ and $z_\psi + 2^{k-4}$ define the same component; hence the number of distinct components ψ_V which are compatible with the system is only $n_{k-2}(z_\chi)/4$. Moreover, the system does not fix the parity of ψ so that both the choices for ψ_U are possible. Concluding, there are $2 \cdot n_{k-2}(z_\chi)/4$ characters ψ whose Gauss sum is equal to that of χ.

Suppose that $u_\chi = -1$ and that ψ and χ have equal parity. Then $\delta = 0$ as before, so that the previous argument proves that there are $n_{k-2}(z_\chi)$ possible values for z_ψ, and $n_{k-2}(z_\chi)/4$ choices for the component ψ_V of ψ. Now suppose that ψ and χ have different parities. Then $\delta = 1$ so that there are $n'_{k-2}(z_\chi)$ choices for z_ψ that (as before) produce $n'_{k-2}(z_\chi)/4$ choices for ψ_V. In both cases the parity of ψ is fixed by that of χ, i.e. ψ_U is fixed by χ_U, therefore the number of characters ψ having Gauss sum equal to that of χ is $n_{k-2}(z_\chi)/4 + n'_{k-2}(z_\chi)/4 = n_{k-3}(z_\chi)/2$, by Proposition 3.

Formula for $|W(\chi)|$. To have equal signatures it is necessary to have equal Gauss sums, hence (5) must be satisfied again. Suppose that $u_\chi = -1$; then $\chi(u_\chi) = \psi(u_\psi)$ because equal signatures imply equal parities. Suppose that $u_\chi = 1$. Then the equality $\chi(u_\chi) = \psi(u_\psi)$ is evident. It follows that the characters ψ whose signature is equal to that of χ are the characters satisfying

$$\begin{cases} \chi(-1) = \psi(-1), \\ u_\chi = u_\psi, \\ F(z_\chi) = F(z_\psi) \pmod{2^{k-2}}. \end{cases}$$

An argument similar to the one we employed for Gauss sums proves that there are $n_{k-2}(z_\chi)/4$ characters satisfying this system. ∎

Example. Let $k = 8$ and let χ be defined by $\chi(-1) = 1$, $\chi(5) = e(9/64)$. Then $a_\chi = 9$ so that $u_\chi = 1$, $v_\chi = 9$, $\rho_\chi = 6$, $z_\chi = 2$, $\nu_0 = 1$, $n_{k-2}(2) = 16$; hence there are eight characters ψ with $\tau(\psi) = \tau(\chi)$ and four characters ψ with $s(\psi) = s(\chi)$.

Example. Let $k = 8$ and let χ be defined by $\chi(-1) = 1$, $\chi(5) = e(31/64)$. Then $a_\chi = 31$ so that $u_\chi = -1$, $v_\chi = -31$, $\rho_\chi = 8$, $z_\chi = -8$, $\nu_0 = 5$, $n_{k-3}(-8) = n_{k-2}(-8) = 8$; hence there are four characters ψ with $\tau(\psi) = \tau(\chi)$ and two characters ψ with $s(\psi) = s(\chi)$.

Proof of Theorem 2. Gauss sums. We write the number of distinct Gauss sums as $\sum_{\{(\mathcal{P},u,z)\}/\sim} 1$, where triplets $(\mathcal{P}_1, u_1, z_1)$ and $(\mathcal{P}_2, u_2, z_2)$ are equivalent when the Gauss sums of the characters χ_1 and χ_2 associated with these triplets are equal. By Proposition 1, the equivalence implies the equality of u_1 and u_2, so we can write the previous sum as $\sum_{\{(\mathcal{P},1,z)\}/\sim} 1 + \sum_{\{(\mathcal{P},-1,z)\}/\sim} 1$; we proceed to the separate evaluation of these sums.

According to Proposition 1, $(\mathcal{P}_1, 1, z_1) \sim (\mathcal{P}_2, 1, z_2)$ iff $\digamma(z_1) = \digamma(z_2) \pmod{2^{k-2}}$; in particular, parities do not matter. It follows that the first sum is equal to the number of distinct values for $\digamma$. By Proposition 2 we can compute this number by taking the sum, over the set of possible values for ν_0, of the quotient of the cardinality of the set of z modulo 2^{k-2} for which $2^{\nu_0} \parallel (z - z_0)$, and the number $n_{k-2}(z)$, hence

$$\text{(6)} \qquad \sum_{\{(\mathcal{P},1,z)\}/\sim} 1 = \sum_{\nu_0=0}^{\lfloor (k-2)/2\rfloor -2} \frac{2^{k-\nu_0-3}}{2^{3+\nu_0}} + \frac{2^{k-(\lfloor (k-2)/2\rfloor -2)-3}}{2^{\lfloor (k-1)/2\rfloor}}$$
$$= \sum_{\substack{j=k-2\lfloor k/2\rfloor \\ j=k \,(\mathrm{mod}\, 2)}}^{k-6} 2^j + 2 = \frac{2^{k-3} + 9 + (-1)^k}{6}.$$

Moreover, according to Proposition 1, $(\mathcal{P}_1, -1, z_1) \sim (\mathcal{P}_2, -1, z_2)$ iff either

$$\begin{cases} \digamma(z_1) = \digamma(z_2) \pmod{2^{k-2}}, \\ \mathcal{P}_1 = \mathcal{P}_2, \end{cases}$$

or

$$\begin{cases} \digamma(z_1) = \digamma(z_2) + 2^{k-3} \pmod{2^{k-2}}, \\ \mathcal{P}_1 = -\mathcal{P}_2. \end{cases}$$

It follows that by Propositions 2 and 3 we can compute the second sum by taking the sum, over the parities and over the set of possible values for ν_0, of the quotient of the number of z modulo 2^{k-2} for which $2^{\nu_0} \parallel (z - z_0)$, and the number $n_{k-2}(z) + n'_{k-2}(z) = 2n_{k-3}(z)$. Since the quantity $2n_{k-3}(z)$ is independent of the parity, the sum over the parities can be computed separately and produces a simple factor 2. Summarizing, we get

$$\text{(7)} \qquad \sum_{\{(\mathcal{P},-1,z)\}/\sim} 1 = 2\Bigg[\sum_{\nu_0=0}^{\lfloor (k-3)/2\rfloor -2} \frac{2^{k-\nu_0-3}}{2^{4+\nu_0}} + \frac{2^{k-(\lfloor (k-3)/2\rfloor -2)-3}}{2^{1+\lfloor (k-2)/2\rfloor}} \Bigg]$$
$$= \sum_{\substack{j=k-2\lfloor (k-1)/2\rfloor \\ j=k \,(\mathrm{mod}\, 2)}}^{k-6} 2^j + 4 = \frac{2^{k-4} + 9 - (-1)^k}{3}.$$

Adding (6) to (7) we get the first result.

Signatures. We write the number of distinct signatures as $\sum_{\{(\mathcal{P},u,z)\}/\sim} 1$ where triplets $(\mathcal{P}_1, u_1, z_1)$ and $(\mathcal{P}_2, u_2, z_2)$ are equivalent when the characters χ_1 and χ_2 associated with these triplets have equal signatures. By Proposition 1 and the definition of parity it follows that $(\mathcal{P}_1, u_1, z_1) \sim (\mathcal{P}_2, u_2, z_2)$ iff $\mathcal{P}_1 = \mathcal{P}_2$, $u_1 = u_2$ and $\digamma(z_1) = \digamma(z_2) \pmod{2^{k-2}}$, so that

$$\sum_{\{(\mathcal{P},u,z)\}/\sim} 1 = 4 \sum_{\{z\}/\sim} 1$$

where $z_1 \sim z_2$ iff $F(z_1) = F(z_2) \pmod{2^{k-2}}$. We have already evaluated this sum in (6) and the result immediately follows. ■

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

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

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

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

[6] G. Molteni, *Multiplicity results for the functional equation of the Dirichlet L-functions*, Acta Arith. 145 (2010), 43–70.

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

[8] A. M. Robert, *A Course in p-Adic Analysis*, Grad. Texts in Math. 198, Springer, New York, 2000.

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 (6181)