C. R. Acad. Sci. Paris, Ser. I 334 (2002) 621–624

Théorie des nombres/*Number Theory*

A note on GL_2 converse theorems

A. Diaconu [a], A. Perelli [b], A. Zaharescu [c]

[a] Department of Mathematics, Columbia University, 2990 Broadway, New York, NY 10027, USA

[b] Dipartimento di Matematica, Via Dodecaneso 35, 16146 Genova, Italy

[c] Department of Mathematics, University of Illinois, 1409 W. Green Street, Urbana, IL 61801, USA

Received 13 December 2001; accepted 11 January 2002

Note presented by Hervé Jacquet.

Abstract Weil's well-known converse theorem shows that modular forms $f \in \mathcal{M}_k(\Gamma_0(q))$ are characterized by the functional equation for twists of $L_f(s)$. Conrey–Farmer had partial success at replacing the assumption on twists by the assumption of $L_f(s)$ having an Euler product of the appropriate form. In this Note we obtain a hybrid version of Weil's and Conrey–Farmer's results, by proving a converse theorem for all $q \geqslant 1$ under the assumption of the Euler product and, moreover, of the functional equation for the twists to a single modulus. ***To cite this article: A. Diaconu et al., C. R. Acad. Sci. Paris, Ser. I 334 (2002) 621–624.*** © 2002 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS

Une note sur les théorèmes inverses de GL_2

Résumé Le théorème bien connu de Weil montre que les formes modulaires $f \in \mathcal{M}_k(\Gamma_0(q))$ sont caractérisées par l'équation fonctionnelle des fonctions L tordues attachées à f. Conrey–Farmer ont partiellement réussi à remplacer cette hypothèse par celle où $L_f(s)$ a un produit eulérien. Dans cette Note, on obtient une version hybride des résultats de Weil et de Conrey–Farmer, en prouvant un théorème inverse pour tout $q \geqslant 1$, sous l'hypothèse d'un produit eulérien et de l'équation fonctionnelle pour les fonctions L tordues par rapport à un seul module. ***Pour citer cet article : A. Diaconu et al., C. R. Acad. Sci. Paris, Ser. I 334 (2002) 621–624.*** © 2002 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS

1. Introduction

In this Note we obtain a kind of hybrid version of Weil's [5] and Conrey–Farmer's [1] converse theorems. In fact, we prove a converse theorem for all $q \geqslant 1$ under the assumption of the Euler product and, moreover, of the functional equation for the twists by all primitive characters to a *single* suitable prime modulus r. We keep the prototypical case considered by Conrey–Farmer, although a similar result can certainly be proved in more general GL_2 situations. We follow the notation in Iwaniec's book [4] and in Conrey–Farmer [1]. Moreover, for a given primitive character χ modulo a prime r with $(q,r)=1$, we consider the functional equation

$$\Lambda_f(s,\chi) = \pm \mathrm{i}^k w(\chi) \Lambda_f(k-s,\overline{\chi}), \tag{1.1}$$

where $\pm$ is the sign of the functional equation satisfied by $L_f(s)$. Our result is

E-mail addresses: cad@math.columbia.edu (A. Diaconu); perelli@dima.unige.it (A. Perelli); zaharesc@math.uiuc.edu (A. Zaharescu).

S1631-073X(02)02277-X/FLA

THEOREM. – *Let $q, k \geqslant 1$ be integers, k even. Suppose $\Lambda_f(s)$ is* EBV *and $L_f(s)$ satisfies both a functional equation and an Euler product of degree* 2, *level q and weight k. Suppose further that for a prime r in a suitable arithmetic progression* (*depending on the algebraic structure of the group $\Gamma_1(q)$*) *a* $\pmod{qc}$ *with* $(qc, a) = 1$ *and for any primitive character χ* $\pmod r$, *$\Lambda_f(s, \chi)$ is* EBV *and satisfies the functional equation* (1.1). *Then $f \in \mathcal{S}_k(\Gamma_0(q))$.*

We remark that a and c are effectively computable. We refer to Section 3 for a simple algorithm for finding a and c starting from a given set of generators of $\Gamma_1(q)$, and for an upper bound on r.

2. Proof of the theorem

Throughout the proof we use the slash operator of weight k extended to the group algebra $\mathbb{C}[\mathrm{GL}_2^+(\mathbb{R})]$ by linearity, i.e., $f|_\gamma = \sum_j a_j f|_{\gamma_j}$ if $\gamma = \sum_j a_j \gamma_j$. Let $T = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $W = W_q = \left(\begin{smallmatrix}1&0\\q&1\end{smallmatrix}\right)$. Recall that $f_{|T} = f$ trivially, and by Hecke's theory it is well known that $f_{|\omega} = \pm f$ and $f_{|W} = f$, since $L_f(s)$ satisfies a functional equation of degree 2, level q and weight k. For $p \nmid q$, the Hecke operator T_p is defined by

$$T_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} + \sum_{b=0}^{p-1} \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix},$$

and $f_{|T_p} = a_p f$ since $L_f(s)$ has an Euler product of degree 2, level q and weight k. See, e.g., Lemma 1 of [1]. Further, any $\gamma_0 \in \Gamma_0(q)$ can be decomposed as follows: for every $t, s \in \mathbb{Z}$

$$\gamma_0 = \begin{pmatrix} a_0 & b_0 \\ qc_0 & d_0 \end{pmatrix} = \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} m & -b \\ -qc & d \end{pmatrix} \begin{pmatrix} 1 & -s \\ 0 & 1 \end{pmatrix}, \tag{2.1}$$

with $m = a_0 + qc_0 t$, $d = d_0 + qc_0 s$, $c = -c_0$ and $-b = b_0 + ms + d_0 t$; see p. 130 of [4]. In view of (2.1), for any $m, b, c, d \in \mathbb{Z}$ with $m \neq 0$ and $md - bqc = 1$ we write

$$\gamma\left(\frac{b}{m}\right) = \begin{pmatrix} m & -b \\ -qc & d \end{pmatrix} \in \Gamma_0(q). \tag{2.2}$$

Note that given m, b with $(m, qb) = 1$ there exist c, d such that $\gamma(\frac{b}{m}) \in \Gamma_0(q)$; we denote by $\gamma(\frac{b}{m})$ any such matrix. Finally, for $x \in \mathbb{R}$ we write $\alpha(x) = \left(\begin{smallmatrix}1&x\\0&1\end{smallmatrix}\right)$ and $\beta(\frac{b}{m}) = (1 - \gamma(\frac{b}{m}))\alpha(\frac{b}{m})$. We need some lemmas.

LEMMA 1 (Weil). – *Let r be a prime with $(q, r) = 1$. Suppose $L_f(s, \chi)$ satisfies* (1.1) *for any primitive character χ* $\pmod r$. *Then $f_{|\beta(b/r)}$ does not depend on b for $(b, r) = 1$.*

Proof. – This is a special case of Lemma 7.9 of [4]. □

Let m be a non-zero integer with $(q, m) = 1$ and let b run over a set of reduced residues modulo m. For each b choose any matrix $\gamma(\frac{b}{m})$ as above, and consider its d-coefficient in (2.2). We denote by D the product of such d-coefficients, as b runs over a set of reduced residues modulo m. With this notation we have

LEMMA 2 (Conrey–Farmer). – *Let m be a non-zero integer with $(q, m) = 1$ and b run over a set of reduced residues* $\pmod m$. *Suppose $f_{|T} = f$, $f_{|\omega} = \pm f$ and for each $p|D$, $f_{|T_p} = \xi_p f$ with some $\xi_p \in \mathbb{C}$. Then $\sum_b' f_{|\beta(b/m)} = 0$, where b runs over the set of reduced residues* $\pmod m$.

Proof. – This is Corollary 2 of [1]. □

Let r be as in Lemma 1. From Lemmas 1 and 2 we deduce that $f_{|\beta(b/r)} = 0$, and hence

$$f_{|\gamma(b/r)} = f \quad \text{for any } (r, b) = 1, \tag{2.3}$$

since $\beta(\frac{b}{r}) = (1 - \gamma(\frac{b}{r}))\alpha(\frac{b}{r})$ and $\alpha(\frac{b}{r})$ is a translation.

We denote by H the group of $\gamma \in SL_2(\mathbb{Z})$ such that $f_{|\gamma} = f$. Clearly, T and W belong to H. Moreover, by (2.3), $\gamma(\frac{b}{r})$ belongs to H for any $(r, b) = 1$. Our aim is to show that $\Gamma_0(q) \subset H$.

LEMMA 3. – *Let m be a non-zero integer with $(q,m)=1$ and suppose $\Gamma_1(q)\subset H$. Then $f_{|\gamma(b/m)}$ does not depend on b for $(m,b)=1$.*

Proof. – Let b, b' be coprime with m. We want to show that $f_{|\gamma(b/m)}=f_{|\gamma(b'/m)}$. In fact,

$$\gamma\left(\frac{b'}{m}\right)\gamma\left(\frac{b}{m}\right)^{-1}=\begin{pmatrix} md-qb'c & mb-b'm\\ q(cd'-c'd) & -qbc'+md'\end{pmatrix}=\gamma$$

with $md-qb'c$, $-qbc'+md'\equiv 1\pmod q$, and hence $\gamma\in\Gamma_1(q)$. The result follows at once. □

PROPOSITION. – *If $\Gamma_1(q)\subset H$ then $\Gamma_0(q)\subset H$.*

Proof. – Let $\gamma_0\in\Gamma_0(q)$. Clearly, by Dirichlet's theorem we can choose t in (2.1) in such a way that $m=p$, p prime with $(q,p)=1$. Accordingly, we have the decomposition

$$\gamma_0=T^{-t}\gamma\left(\frac{b}{p}\right)T^{-s} \tag{2.4}$$

for some b. Writing $R_p=\sum_a'\alpha(\frac{a}{p})$, by Lemmas 2 and 3 we have

$$f_{|(1-\gamma(b/p))R_p}=0. \tag{2.5}$$

Denoting by I the 2×2 identity matrix, a computation shows that

$$I+2R_p+R_p^2=(I+R_p)^2=\sum_{a,a'=1}^{p}\alpha\left(\frac{a+a'}{p}\right)=p(I+R_p),$$

and hence $I=R_p(\frac{1}{p-1}R_p-\frac{p-2}{p-1}I)$. Applying $\frac{1}{p-1}R_p-\frac{p-2}{p-1}I$ to the right of both sides of (2.5) we therefore get $f_{|\gamma(b/p)}=f$, and the result follows by (2.4). □

Now we are ready for the proof of the theorem. In view of the proposition, it suffices to prove that $f_{|\gamma}=f$ for every $\gamma\in\Gamma_1(q)$. Let

$$\gamma_j=\begin{pmatrix} a_j & b_j\\ qc_j & d_j\end{pmatrix},\quad j=1,\dots,h, \tag{2.6}$$

be a set of generators of $\Gamma_1(q)$. It is enough to prove that $f_{|\gamma_j}=f$ for $j=1,\dots,h$. We first show that if $\gamma_1,\dots,\gamma_h$ are any set of matrices in $\Gamma_1(q)$ of the form (2.6) with entries satisfying

$$(q,c_1\cdots c_h)=1\quad\text{and}\quad (c_i,c_j)=1\quad\text{for } i\neq j, \tag{2.7}$$

then $f_{|\gamma_j}=f$ for $j=1,\dots,h$. To this end, consider the system

$$x\equiv a_j\ \bigl(\mathrm{mod}\ q|c_j|\bigr),\quad j=1,\dots,h, \tag{2.8}$$

and note that every solution of the system

$$\begin{cases} x\equiv a_j\ (\mathrm{mod}\ |c_j|), & j=1,\dots,h,\\ x\equiv 1\ (\mathrm{mod}\ q)\end{cases} \tag{2.9}$$

is a solution of (2.8) as well. In fact, $a_j\equiv 1\pmod q$ for $j=1,\dots,h$ since $\gamma_j\in\Gamma_1(q)$. Moreover, by the chinese remainder theorem, the system (2.9) has a solution a $(\mathrm{mod}\ q|c_1\cdots c_h|)$ with some $(a,qc_1\cdots c_h)=1$. Therefore, by Dirichlet's theorem there exists a prime r with $(q,r)=1$ satisfying (2.8). Then, in view of the expression of m in (2.1), by the decomposition (2.1) there exist integers t_j,s_j and b_j' with $(r,b_j')=1$ such that

$$\gamma_j=T^{-t_j}\gamma\left(\frac{b_j'}{r}\right)T^{-s_j},\quad j=1,\dots,h. \tag{2.10}$$

Hence, supposing that such an r is the prime referred to in the theorem (which is consistent, since r belongs to a progression of type a modulo qc with $(a,qc)=1$), by (2.3) we get $f_{|\gamma_j}=f$ for $j=1,\dots,h$.

It is therefore left to show that the generators of $\Gamma_1(q)$ can be suitably linked to matrices satisfying (2.7). To this end we note the following identity in $\mathrm{SL}_2(\mathbb{Z})$

$$\omega\begin{pmatrix} a & b \\ qc & d \end{pmatrix}\omega^{-1} = \begin{pmatrix} d & -c \\ -qb & a \end{pmatrix}. \tag{2.11}$$

Next we observe that if γ_j, $j = 1, \ldots, h$, are the generators in (2.6) and $t_j \in \mathbb{Z}$, then

$$\gamma_j T^{t_j} = \begin{pmatrix} a_j & a_j t_j + b_j \\ qc_j & qc_j t_j + d_j \end{pmatrix} \in \Gamma_1(q), \quad j = 1, \ldots, h.$$

Moreover, since $(a_j, b_j) = 1$, by Dirichlet's theorem we can choose the t_j's in such a way that $a_j t_j + b_j = p_j =$ prime, $p_i \neq p_j$ and $(q, p_j) = 1$. Writing $l_j = qc_j t_j + d_j$ we have $\gamma_j T^{t_j} = \left(\begin{smallmatrix} a_j & p_j \\ qc_j & l_j \end{smallmatrix}\right)$ for $j = 1, \ldots, h$, and hence by (2.11)

$$\omega\gamma_j T^{t_j}\omega^{-1} = \begin{pmatrix} l_j & -c_j \\ -qp_j & a_j \end{pmatrix} = \gamma'_j \in \Gamma_1(q), \quad j = 1, \ldots, h, \tag{2.12}$$

say. Thus the entries of each γ'_j satisfy the coprimality conditions in (2.7) and hence $f_{|\gamma'_j} = f$ for $j = 1, \ldots, h$.

In conclusion, from (2.12) we have that the generators $\gamma_1, \ldots, \gamma_h$ satisfy $\gamma_j = \omega^{-1}\gamma'_j\omega T^{-t_j}$, $j = 1, \ldots, h$, with $\gamma'_j \in H$, and hence $\Gamma_1(q) \subset H$. Finally, the assertion that $f \in \mathcal{S}_k(\Gamma_0(q))$ is verified by the same argument in the proof of Corollary 1 of [1], and the theorem is proved.

3. An algorithm

We first note that the prime r referred to in the theorem can be obtained by applying the procedure leading to (2.10) to the matrices γ'_j in (2.12) in place of the matrices γ_j in (2.6). Moreover, the numbers p_j in (2.12) do not need to be primes, the important property being that the entries of the matrices γ'_j satisfy conditions (2.7). A simple algorithm to find the required prime r starting from a given set of generators of $\Gamma_1(q)$ can be described as follows.

Let γ_j, $j = 1, \ldots, h$, be a set of generators of $\Gamma_1(q)$ with entries given by (2.6), and suppose that $|a_j| \leqslant A$ for $j = 1, \ldots, h$. Choose p_1 to be the least positive integer satisfying $p_1 \equiv b_1 \pmod{a_1}$ and $(q, p_1) = 1$. Next choose p_2 to be the least positive integer satisfying $p_2 \equiv b_2 \pmod{a_2}$ and $(qp_1, p_2) = 1$, then p_3 with $p_3 \equiv b_3 \pmod{a_3}$ and $(qp_1p_2, p_3) = 1$ and so on. Thus we get matrices γ'_j as in (2.12), with $(q, p_1 \cdots p_h) = 1$ and $(p_i, p_j) = 1$ for $i \neq j$. By sieve theory (*see* Theorem 8.4 of Halberstam–Richert [2]) it follows that for any fixed $\varepsilon > 0$ one has

$$p_j \ll_{h,\varepsilon} q^\varepsilon A^{1+\varepsilon}, \quad j = 1, \ldots, h, \tag{3.1}$$

where the implied constant is effectively computable in terms of h and ε. Now we consider the system (2.9) with $a_j = l_j$ and $c_j = p_j$, $j = 1, \ldots, h$, and its solution $a \pmod{qc}$, where $c = p_1 \cdots p_h$. The required prime r can therefore be chosen as the least prime in the progression $a \pmod{qc}$. In view of Heath–Brown's [3] bound $\mathrm{O}(q^{5.5})$ for the least prime in an arithmetic progression $\pmod{q}$, by (3.1) we have the bound

$$r \ll_{h,\varepsilon} \left(qA^h\right)^{5.5+\varepsilon}.$$

References

[1] J.B. Conrey, D.W. Farmer, An extension of Hecke's converse theorem, Internat. Math. Res. Notices (1995) 445–463.

[2] H. Halberstam, H.-E. Richert, Sieve Methods, Academic Press, 1974.

[3] D.R. Heath-Brown, Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression, Proc. London Math. Soc. (3) 64 (1992) 265–338.

[4] H. Iwaniec, Topics in Classical Automorphic Forms, American Mathematical Society, 1997.

[5] A. Weil, Über die Bestimmung Dirichletscher Reihen durch Funktionengleichungen, Math. Ann. 168 (1967) 149–156.