Gaussian Sums over $GL(2, \mathbf{Z}/N)$ and Hecke Operators I

ROY J. FULLER

Communicated by the Editors

If R is a representation of $GL(2, \mathbf{Z}/N)$ and A is a matrix in $M(2, \mathbf{Z})$, then the Gaussian sum $W(A)$ is defined by

$$W(A) = \sum_g R(g) \exp [2\pi i \operatorname{trace} (Ag)/N]$$

where g is summed over $GL(2, \mathbf{Z}/N)$. These Gaussian sums lead to a Hecke operator which acts on automorphic forms "of type R ," which appeared, in a more general setting, in Shimura's paper [2], where it was suggested that the associated Dirichlet series might have an Euler product. Our goal is to calculate the " p factor" of the Euler product for the prime divisors of N . The main result is Proposition 6.

1. We begin by reviewing some definitions from [2], making the appropriate specializations. R will denote an irreducible representation of $GL(2, \mathbf{Z}/N)$ by complex matrices of size d . We always suppose that R is primitive, *i.e.*, R is not obtained by composing a representation of $GL(2, \mathbf{Z}/M)$ with the natural homomorphism $GL(2, \mathbf{Z}/N) \rightarrow GL(2, \mathbf{Z}/M)$, where M is a proper divisor of N . Let $\mathbf{C}^+ = \{z \mid \operatorname{Im}(z) > 0\}$ denote the upper half of the complex plane, and let $\mathbf{C}^d$ denote the space of complex column vectors of dimension d . For each function

$$f : \mathbf{C}^+ \rightarrow \mathbf{C}^d \quad \text{and each} \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{in} \quad M(2, \mathbf{Z})$$

such that $\det(A) > 0$, we have the A -transform $f \mid A$ of weight k :

$$(f \mid A)(z) = \det(A)^{k/2} (cz + d)^{-kf} ((az + b)/(cz + d)).$$

f is a *cuspidal form of type (R, k)* if the following conditions are satisfied:

(1) The coordinate functions of f are all cusp forms of weight k with respect to the principal congruence subgroup $\Gamma_N = \{A \in \Gamma \mid A \equiv I \pmod{N}\}$.

(2) $(f \mid A)(z) = R(A)f(z)$ for all A in $\Gamma = SL(2, \mathbf{Z})$.

$S(R, k)$ will denote the space of cusp forms of type (R, k) .

The Hecke operators $T(A)$ are defined as follows: given A in $M(2, \mathbf{Z})$, one can express $\Gamma A \Gamma$ as the finite disjoint union of right cosets ΓA_i . Given f in $S(R, k)$, if $\det(A) > 0$, put

$$(1) \quad f | T(A) = \sum_i W(A_i)(f | A_i).$$

The right side of (1) is independent of the choice of coset representatives A_i , and determines an element of $S(R, k)$. The associated Dirichlet series is

$$\mathfrak{W}(s) = \sum T(A) (\det A)^{-s}$$

summed over all $\Gamma A \Gamma$ such that $\det(A)$ is a product of the primes which divide N and is positive.

The next step is to express $\mathfrak{W}(s)$ as a product $\prod_{p|N} \mathfrak{W}(s, p)$. The group $GL(2, \mathbf{Z}/N)$ is naturally isomorphic to the (external) direct product $\prod_{p|N} GL(2, \mathbf{Z}/p^n)$, corresponding to the prime factorization of the integer N . (Here n depends on p , but our notation should not create confusion.) We prefer to deal with an internal direct product, so let us agree to identify $GL(2, \mathbf{Z}/p^n)$ with its image in $GL(2, \mathbf{Z}/N)$. Thus each matrix g of $GL(2, \mathbf{Z}/N)$ is uniquely expressible as a product $\prod g_p$, where g_p is in the image of $GL(2, \mathbf{Z}/p^n)$, and the factors g_p commute with each other. Furthermore, $R(g) = \prod R(g_p)$, and the matrices $R(g_p)$ commute with each other. Put $R_p(g) = R(g_p)$. R_p is thus the representation obtained by the following composition:

$$GL(2, \mathbf{Z}/N) \rightarrow GL(2, \mathbf{Z}/p^n) \rightarrow GL(2, \mathbf{Z}/N) \xrightarrow{R} GL(d, \mathbf{C}).$$

Moreover, if A is in $M(2, \mathbf{Z})$ and $\det(A)$ is not divisible by p , then A determines an element of $GL(2, \mathbf{Z}/p^n)$, which we identify with an element of $GL(2, \mathbf{Z}/N)$. That element we denote A_p . A_p is the solution of the simultaneous congruences:

$$A_p = A \pmod{p^n}$$

$$A_p = I \pmod{q^*} \text{ other primes } q \text{ dividing } N.$$

Here q^* denotes the highest power of q which divides N . In this case, $R_p(A)$ is meaningful, and it means $R(A_p)$.

We can select integers a_p , one for each prime divisor of N , so that

$$1/N = \sum_{p|N} (a_p/p^n).$$

a_p is unique modulo p^n . Then define $W(A, p)$ by

$$W(A, p) = \sum_g R_p(g) \exp [2\pi i a_p \text{trace}(Ag)/p^n]$$

where g is summed over $GL(2, \mathbf{Z}/p^n)$.

Proposition 0. $W(A) = \prod_{p|N} W(A, p)$ and the factors $W(A, p)$ commute with each other.

Proof. For fixed g we have

$$\begin{aligned}\exp [2\pi i \operatorname{trace} (Ag)/N] &= \prod_{p|N} \exp [2\pi i a_p \operatorname{trace} (Ag)/p^n] \\ &= \prod_{p|N} \exp [2\pi i a_p \operatorname{trace} (Ag_p)/p^n].\end{aligned}$$

We have used the trick of replacing g by g_p in the p -th factor, which is permitted because the two are congruent modulo p^n . Next:

$$R(g) \exp [2\pi i \operatorname{trace} (Ag)/N] = \prod_{p|N} R(g_p) \exp [2\pi i a_p \operatorname{trace} (Ag_p)/p^n].$$

Summing over g in $GL(2, \mathbf{Z}/N)$:

$$\begin{aligned}W(A) &= \sum_g \prod_{p|N} R(g_p) \exp [2\pi i a_p \operatorname{trace} (Ag_p)/p^n] \\ &= \prod_{p|N} \sum_{g_p} R(g_p) \exp [2\pi i a_p \operatorname{trace} (Ag_p)/p^n] \\ &= \prod_{p|N} W(A, p).\end{aligned}$$

The factors $W(A, p)$ commute because the matrices $R(g_p)$ commute with each other. Q.E.D.

If $\det(A)$ is a power of p , define $W(A, p)'$ by

$$W(A, p)' = W(A, p) \prod_q R_q(A)^{-1}$$

where q runs over the prime divisors of N , omitting p . The essential difference between $W(A, p)'$ and $W(A, p)$ lies in the identities:

$$\begin{aligned}W(BAC, p) &= R_p(C)^{-1} W(A, p) R_p(B)^{-1}, \\ W(BAC, p)' &= R(C)^{-1} W(A, p)' R(B)^{-1}.\end{aligned}$$

(Here B and C must be such that the above expressions are well defined.)

The operator $T(A, p): S(R, k) \rightarrow S(R, k)$ is defined whenever $\det(A)$ is a power of p by

$$f | T(A, p) = \sum W(A_i, p)' (f | A_i)$$

where the A_i run over a set of representatives for the cosets ΓA_i which are contained in $\Gamma A \Gamma$. Finally, the Dirichlet series $\mathfrak{W}(s, p)$ is defined by

$$\mathfrak{W}(s, p) = \sum T(A, p) \det(A)^{-s}$$

summed over all the $\Gamma A \Gamma$ such that $\det(A)$ is a power of p . As we said, these are specializations of some definitions from [2]. Our goal to calculate an explicit rational expression for $\mathfrak{W}(s, p)$.

Proposition 1. *Let the distinct prime divisors of N be $p_1, \dots, p_m$. Let B_i be a matrix in $M(2, \mathbf{Z})$ with positive determinant which is a power of p_i . Then:*

$$(1) \quad W(B_1 \cdots B_m) = W(B_m, p_m)' \cdots W(B_1, p_1)'.$$

(2) $T(B_1 \cdots B_m) = T(B_m, p_m) \cdots T(B_1, p_1)$, and the factors on the right commute with each other.

(3) $\mathfrak{W}(s) = \mathfrak{W}(s, p_m) \cdots \mathfrak{W}(s, p_1)$, and the factors on the right side commute with each other.

Proof. (1) It is sufficiently general to take the case

$$\begin{aligned}
 m = 3 : W(B_1 B_2 B_3) &= W(B_1 B_2 B_3, p_1) W(B_1 B_2 B_3, p_2) W(B_1 B_2 B_3, p_3) \\
 &= R_{p_1}(B_3)^{-1} R_{p_1}(B_2)^{-1} W(B_1, p_1) R_{p_2}(B_3)^{-1} W(B_2, p_2) R_{p_3}(B_1)^{-1} \\
 &\quad \cdot W(B_3, p_3) R_{p_3}(B_2)^{-1} R_{p_3}(B_1)^{-1} \\
 &= R_{p_1}(B_3)^{-1} R_{p_2}(B_3)^{-1} W(B_3, p_3) R_{p_1}(B_2)^{-1} W(B_2, p_2) R_{p_3}(B_2)^{-1} \\
 &\quad \cdot W(B_1, p_1) R_{p_3}(B_1)^{-1} R_{p_3}(B_1)^{-1} \\
 &= W(B_3, p_3)' W(B_2, p_2)' W(B_1, p_1)'.
 \end{aligned}$$

We used the fact that R_{p_1} , R_{p_2} , and R_{p_3} commute with each other. (It is not permitted to commute, say, $R_{p_1}(B_2)$ and $W(B_1, p_1)$, however.)

(2) It is a basic fact of modular correspondence theory [3] that whenever $\det(B_i)$ ($i = 1, \dots, m$) are pairwise relatively prime, then coset representatives for $\Gamma B_1 \cdots B_m \Gamma$ may be found by choosing representatives for the cosets $\Gamma B_i^{(i)}$ contained in $\Gamma B_i \Gamma$, and then forming the products $B_1^{(i_1)} \cdots B_m^{(i_m)}$. Thus

$$\begin{aligned}
 f \mid T(B_1, p_1) \cdots T(B_m, p_m) \\
 &= \sum W(B_m^{(i_m)}, p_m)' \cdots W(B_1^{(i_1)}, p_1)' f \mid (B_1^{(i_1)} \cdots B_m^{(i_m)}) \\
 &= \sum W(B_1^{(i_1)} \cdots B_m^{(i_m)}) f \mid (B_1^{(i_1)} \cdots B_m^{(i_m)}) \\
 &= f \mid T(B_1 \cdots B_m).
 \end{aligned}$$

The operators $T(B_i, p_i)$ commute with each other because $T(B_1 \cdots B_m)$ depends only on the set $\Gamma B_1 \cdots B_m \Gamma$, and that set is independent of the ordering of the factors B_i in the case where the determinants of the B_i are pairwise relatively prime.

(3) follows immediately from (2).

Q.E.D.

2. We are going to calculate an explicit rational expression for $\mathfrak{W}(s, p)$ for a certain class of representations R . First, we want to examine how the representation R_p splits into irreducible components.

Proposition 2. *If R is irreducible, then R_p contains, up to equivalence, only one irreducible representation of $GL(2, \mathbf{Z}/p^n)$.*

Proof. R is equivalent to a Kronecker product $\bigotimes_{a \mid N} (r_a)$ where r_a is an irreducible representation of $GL(2, \mathbf{Z}/q^m)$. Evidently, R_p is equivalent to $r_p \bigotimes I = r_p \bigoplus \cdots \bigoplus r_p$.

Q.E.D.

Proposition 3. $T(A, p) = 0$ if all the entries of A are divisible by p .

Proof. Corresponding to the direct sum $R_p = r_p \oplus \cdots \oplus r_p$, the Gaussian sum $W(A, p)$ splits into a direct sum $w(A, p) \oplus \cdots \oplus w(A, p)$, where $w(A, p) = \sum_g r_p(g) \exp [2\pi i a_p \text{trace } (Ag)/p^n]$ with the summation over all g in $GL(2, \mathbf{Z}/p^n)$. It is enough to show that $w(A, p) = 0$. Since we assume that R is primitive modulo N , it follows that r_p is primitive modulo p^n . Therefore, $w(A, p)$ vanishes if all the entries of A are divisible by p . [1] **Q.E.D.**

The sets $\Gamma A \Gamma$ such that $\det(A)$ is a power of p have as canonical representatives the diagonal matrices $A = \text{diag } (p^x, p^y)$, $x \leq y$. With the vanishing of $T(A, p)$ for $1 \leq x \leq y$, the series $\mathfrak{W}(s, p)$ reduces to summation only over the diagonal matrices $\text{diag } (1, p^y)$. If we denote $T(\text{diag } (1, p^y), p)$ by simply $T(y, p)$, then we have

$$\mathfrak{W}(s, p) = \sum_{y=0}^{\infty} T(y, p) p^{-ys}.$$

Proposition 4. Let $G_0(p)$ denote the subgroup of $GL(2, \mathbf{Z}/p^n)$ consisting of all g such that $gA_0 = A_0$, where $A_0 = \text{diag } (1, p^n)$. If the restriction of r_p to $G_0(p)$ contains no trivial representation, then $T(y, p) = 0$ for $y \geq n$, and thus $\mathfrak{W}(s, p)$ is a polynomial in p^{-s} .

Proof. We have

$$w(A_0, p) = \sum_h r_p(h) \exp [2\pi i a_p \text{trace } (A_0 h)/p^n] (\sum_g r_p(g))$$

where the summations are over all g in $G_0(p)$, and over a set of representatives h for the left cosets $hG_0(p)$ in $GL(2, \mathbf{Z}/p^n)$. If the restriction of r_p to $G_0(p)$ contains no trivial representation, then the sum over g vanishes; hence, $w(A_0, p) = 0$, hence, $T(y, p) = 0$ for $y \geq n$. **Q.E.D.**

There remain the primitive irreducible representations r_p which contain a trivial representation when restricted to $G_0(p)$. These are in one-one correspondence with the characters of a reduced residue system modulo p^n [1]. The character ϕ corresponding to r_p can be recovered from the action of r_p on scalar matrices: $r_p(xI) = \phi(x)^{-1} r_p(I)$. When ϕ is a primitive character modulo p^n , the Gaussian sums $w(A, p)$ satisfy the following identity [1]:

$$w(A, p)w(B, p) = cw(BA, p).$$

The complex number c depends on $p^a = \det(A)$, and $p^b = \det(B)$, as follows: Put $\lambda = -w(\phi^{-1})p^{2n-1}$ where

$$w(\phi^{-1}) = \sum_x \phi(x)^{-1} \exp (2\pi i a_p x/p^n)$$

is the ordinary Gaussian sum of the character ϕ^{-1} modulo p^n . Then

$$\text{If } n = 1 : c = \lambda \quad \text{if } a = 0 \quad \text{or } b = 0,$$

$$c = -(p-1)\lambda \quad \text{if } a > 0 \quad \text{and } b > 0.$$

$$\begin{aligned}
\text{If } n > 1 : c &= -\lambda/(p-1) \quad \text{if } a = n-1, b = n-1, \\
c &= \lambda \quad \text{if } a = n, b = n-1, \quad \text{or} \\
a &= n-1, b = n, \\
c &= -\lambda(p-1) \quad \text{if } a \geq n, b \geq n, \\
W(A, p) &= 0 \quad \text{if } 0 \leq a \leq n-2.
\end{aligned}$$

$W(A, p)$ satisfies the same identities as $w(A, p)$, and so does $W(A, p)'$, for it is obtained from $W(A, p)$ by multiplying by the factors $R_q(A)^{-1}$.

Proposition 5. *If r_p is one of the representations corresponding to a primitive character modulo p^n , then the operators $T(y, p)$ satisfy the following identities:*

$$\begin{aligned}
n = 1 : (1) \quad & T(0, p) = \lambda \quad \text{times the identity,} \\
(2) \quad & T(a, p)T(b, p) = -(p-1)\lambda T(a+b, p) \quad \text{if } a > 0 \\
& \text{and } b > 0. \\
n > 1 : (3) \quad & T(0, p), \dots, T(n-2, p) \quad \text{all vanish,} \\
(4) \quad & T(n-1, p)^2 = -\lambda(p-1)^{-1}T(2n-2, p), \\
(5) \quad & T(n-1, p)T(b, p) = \lambda T(n-1+b, p), \quad b \geq n, \\
(6) \quad & T(a, p)T(b, p) = -\lambda(p-1)T(a+b, p) \quad a, b \geq n.
\end{aligned}$$

Proof. (1) and (3) are clear, and the others are proved as follows: select coset representatives A_i (resp. B_i) for the cosets ΓA_i (resp. ΓB_i) contained in $\Gamma A \Gamma$ (resp. $\Gamma B \Gamma$) for $A = \text{diag}(1, p^a)$ (resp. $B = \text{diag}(1, p^b)$). From the products $A_i B_j$ we can select a set of representatives for the right cosets ΓC contained in $\Gamma A B \Gamma$, and the remaining $A_i B_j$ will have all entries divisible by p . We have

$$\begin{aligned}
f \mid T(a, p)T(b, p) &= \sum W(B_j, p)' W(A_i, p)' f \mid A_i B_j \\
&= \sum c W(A_i B_j, p)' f \mid A_i B_j.
\end{aligned}$$

$W(A_i B_j, p)'$ vanishes whenever $A_i B_j$ has all entries divisible by p , and when those terms are deleted, what remains is precisely summation over a set of representatives for the right cosets ΓC contained in $\Gamma A B \Gamma$. Hence, $f \mid T(a, p)T(b, p) = c(f \mid T(a+b, p))$. Q.E.D.

Proposition 6. *If r_p is one of the representations corresponding to a primitive character modulo p^n , then $\mathfrak{W}(s, p)$ satisfies the (formal) equation*

$$\mathfrak{W}(s, p) = T(n-1, p)p^{-(n-1)s} \frac{(p-1)T(n-1, p) + T(n, p)p^{-(s-1)}}{(p-1)T(n-1, p) + T(n, p)p^{-s}}.$$

Proof. Multiply $\mathfrak{W}(s, p)$ by $(p-1)T(n-1, p) + T(n, p)p^{-s}$ and apply the identities of Proposition 5. Q.E.D.

REFERENCES

1. R. FULLER, *Gaussian sums over $GL(2, \mathbf{Z}/p^n)$* , Indiana Univ. Math. J. **23** (1974), 1013–1020.
2. G. SHIMURA, *On Dirichlet series and abelian varieties attached to automorphic forms*, Ann. of Math. **76** (1962), 237–294.
3. G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan, No. 11, 1971.

University of Arkansas

Date communicated: JANUARY 14, 1974