MATHEMATICS

1961

SovietRxiv

Abstract

Full Text

MATHEMATICS

A. N. ANDRIANOV

A GENERALIZATION OF A THEOREM OF M. EICHLER FROM THE THEORY OF QUATERNARY QUADRATIC FORMS

(Presented by Academician I. M. Vinogradov on 3 VI 1961)

Let

$$F(x_1, \dots, x_4) = \sum_{1 \le i \le j \le 4} a_{ij} x_i x_j$$

be a positive definite quaternary quadratic form with integral rational and relatively prime coefficients a_{ij}. Then

$$F(x_1, \dots, x_4) = \frac{1}{2} \overline{X} F X,$$

where $\overline{X} = (x_1, \dots, x_4)$ and the letter F denotes the matrix of the form F. Let D and q be, respectively, the discriminant and the level of F; $\mathfrak{C} = (e_1, \dots, e_4)$ an integral solution of the congruence $F\mathfrak{C} \equiv 0 \pmod{q}$; $t = \text{g.c.d.} \left(q, \frac{\overline{\mathfrak{C}} F \mathfrak{C}}{2q}\right)$; $t_1 = \frac{q}{t}$; $\Gamma = \Gamma(q, t_1)$ the group of integral unimodular matrices of the second order $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \equiv 0 \pmod{q}$, $b \equiv 0 \pmod{t_1}$; Γ_0 its subgroup consisting of matrices for which $a \equiv 1 \pmod{q}$. Then the theta series

$$\vartheta_F(\tau|\mathfrak{C}) = \sum_N \exp\left(\pi i t \left(\overline{N} + \frac{\overline{\mathfrak{C}}}{q}\right) F \left(N + \frac{\mathfrak{C}}{q}\right)\right) = \sum_{n=0}^{\infty} a_F(n) \exp\left(\frac{2\pi i t n}{q_1}\right),$$

where the summation is over all integral 4-dimensional vectors $\overline{N} = (n_1, \dots, n_4)$, and where $a_F(n)$ is the number of integral solutions of the equation

$$2qtn = (qX + \mathfrak{C}) F (qX + \mathfrak{C}),$$

is an integral modular form of degree q and dimension -2 for the group Γ_0 ([2]). As Hecke showed ([3]),

$$\vartheta_F(\tau|\mathfrak{C}) = E_F(\tau|\mathfrak{C}) + S_F(\tau|\mathfrak{C}),$$

where $E_F(\tau|\mathfrak{C})$ is an Eisenstein series, and $S_F(\tau|\mathfrak{C})$ is a parabolic form. Let $b_F(n)$ and $d_F(n)$ be the coefficients of

$$\exp\left(\frac{2\pi i t n}{q}\right)$$

in the expansions of the forms $E_F(\tau|\mathfrak{C})$, $S_F(\tau|\mathfrak{C})$; then

$$a_F(n) = b_F(n) + d_F(n).$$

The quantity $b_F(n)$ gives the principal term of the number of solutions of the equation indicated above and is computed without difficulty, while $d_F(n)$ is the remainder term. In the present note the following is proved.

Theorem. There exists a natural number Q such that, for all n relatively prime to Q, the estimate

$$|d_F(n)| \leq c_F \tau(n)\sqrt{n}, \tag{1}$$

holds, where c_F is a constant depending only on F, and $\tau(n)$ is the number of divisors of n.

For $\mathfrak{C} = 0$ this estimate was proved by Eichler ([1]). The method used by us is analogous to Eichler' s method.

Proof. Denote by Λ_{2k} $(k = 1, 2, ...)$ the set of all parabolic forms $F(\tau)$ such that, first,

$$F\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{2k}F(\tau), \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0$$

and, secondly, both $F(\tau)$ itself and the form

$$(c\tau+d)^{-2k}F\left(\frac{a\tau+b}{c\tau+d}\right) \quad \text{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

have rational, almost integral Fourier coefficients (here and below the coefficients of the Fourier expansion in a neighborhood of the point $i\infty$ are meant).

Let us note some properties of Λ_{2k}:

1) Λ_{2k} is nonempty. Indeed, from the properties of theta series and the series $E_F(\tau \mid \mathfrak{E})$ ([2,3]) it follows that, for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$,

$$S_F\left(\frac{a\tau+b}{c\tau+d}\,\middle|\,\mathfrak{E}\right) = \left(\frac{D}{a}\right)(c\tau+d)^2 S_F(\tau \mid a\mathfrak{E}),$$

where $\left(\frac{D}{a}\right)$ is the Kronecker symbol, and that $S_F(\tau \mid \mathfrak{E})$ has rational and almost integral Fourier coefficients. Thus, for $k = 1, 2, ...$, $\left(S_F(\tau \mid \mathfrak{E})\right)^k \in \Lambda_{2k}$.

2) Λ_{2k} is a vector space over the field R of rational numbers; it is finite-dimensional, since the whole space of modular forms for the group Γ_0 of the given dimension $-2k$ is finite-dimensional.

3) On Λ_{2k} the factor group Γ/Γ_0, isomorphic to the multiplicative group of residue classes modulo q relatively prime to q, acts as a group of operators: $R_a : \Lambda_{2k} \to \Lambda_{2k}$, $(a, q) = 1$.

Define on the space Λ_{2k} the Hecke operators $T(m)$ (see ([4])), putting, for $F(\tau) \in \Lambda_{2k}$,

$$F(\tau) \cdot T(m) = m^{2k-1} \sum_{(a,d,b)} F(\tau) R_{a'} \begin{pmatrix} a & bt_1 \\ 0 & d \end{pmatrix},$$

where the summation is over all triples (a, d, b) satisfying the conditions $ad = m$, $a, d > 0$, $(a, q) = 1$, $0 \leq b < d$, where $a'a \equiv 1 \pmod{q}$, and where, for a form $G(\tau) \in \Lambda_{2k}$ and an integral matrix $\begin{pmatrix} l & f \\ p & s \end{pmatrix}$, it is put, for brevity,

$$(p\tau + s)^{-2k} G\left(\frac{l\tau + f}{p\tau + s}\right) = G(\tau) \begin{pmatrix} l & f \\ p & s \end{pmatrix}.$$

It is known ([4]) that

$$(F(\tau) \cdot T(m)) \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (F(\tau) \cdot R_a) T(m) \quad \text{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

and, moreover, that together with $F(\tau)$, $F(\tau) \cdot T(m)$ for any m has rational, almost integral Fourier coefficients; thus $T(m) : \Lambda_{2k} \to \Lambda_{2k}$.

Consider the set K consisting of all functions $f(\tau)$ of the form $f(\tau) = \dfrac{F(\tau)}{G(\tau)}$, where $F(\tau), G(\tau) \in \Lambda_{2k}$, $k = 1, 2, \ldots$. It is clear that K is a field. If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0$, then $f\left(\dfrac{a\tau + b}{c\tau + d}\right) = f(\tau)$, so that K is a subfield of the field of all modular functions with respect to Γ_0, and is the field of algebraic functions of one variable over the field of constants R. Let us note that all functions $f(\tau) \in K$ have rational, almost integral Fourier coefficients.

Let $\overline{K}$ be the field obtained from K by algebraically closing the field of constants. If $(F_i(\tau))$, $i = 1, 2, \ldots, g$, is a basis of the space Λ_2, then $(F_i(\tau)d\tau)$, $i = 1, 2, \ldots, g$, form a basis of the space of integral differentials of the field K, and hence also of $\overline{K}$. Let p be a prime, and let the operator $T(p)$ on Λ_2 be given in the basis $(F_i(\tau))$ by the matrix $T(p)$. Construct a prime multiplier ([6a]) τ_p of the field $\overline{K}$ into itself, which in the basis $\overline{DU} = (F_i(\tau)d\tau)$ is represented by the matrix $T(p)$. If $\overline{K}_0$ is a field abstractly isomorphic to the field $\overline{K}$, then the prime multipliers of the field $\overline{K}$ into itself correspond to isomorphisms of the field $\overline{K}_0$ onto subfields $\overline{K}_0^*$ of finite algebraic extensions $\overline{K}^*$ of the field K ([6a]). Let the field $\overline{K}$ consist of functions $f(\tau)$, and the field $\overline{K}_0$ of functions $y(\tau)$, $y(\tau) \leftrightarrow f(\tau)$;

As $\overline{K}_0^*$ take the field formed by the functions $f\left(\dfrac{\tau}{p}\right)$, and as the isomorphism $\overline{K}_0 \to \overline{K}_0^*$ take the isomorphism carrying $y(\tau)$ into $f\left(\dfrac{\tau}{p}\right)$. Let $\overline{K}^*$ be the

composite of $\overline{K}$ and $\overline{K}_0^*$. It is easy to see that the conjugates of $f\left(\frac{\tau}{p}\right)$ over $\overline{K}$ will be the functions $f\left(\frac{\tau+t_1 r}{p}\right)$, $r=0,1,\dots,p-1$, and $f(\tau)\cdot R_{p'}\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}$, where $p'p\equiv 1 \pmod q$. Thus $[\overline{K}^* : \overline{K}]<\infty$. Let τ_p be the multiplier determined by this isomorphism. Put $\delta u = \left(F_i\left(\frac{\tau}{p}\right) d\left(\frac{\tau}{p}\right)\right)$, $i=1,2,\dots,g$; then to the multiplier τ_p there corresponds the matrix $T^*(p)$, determined from relation (66):

$$\operatorname{Sp}\overline{K}^*/\overline{K}\,(\delta u) = T^*(p)\,du.$$

But since the conjugates of the integral differential $F_i\left(\frac{\tau}{p}\right)d\frac{\tau}{p}$ of the field $\overline{K}^*$ over $\overline{K}$ will be the differentials $F_i\left(\frac{\tau+t_1 r}{p}\right)d\left(\frac{\tau+t_1 r}{p}\right)$, $r=0,1,\dots,p-1$, and $F_i(\tau)\,R_{p'}\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}dp\tau$, it is clear that $T^*(p)=T(p)$.

Besides the multipliers τ_p, the multipliers R_a for $(a,q)=1$ are naturally defined as the multipliers corresponding to automorphisms R_a of the field K, defined as follows: if $f(\tau)=\frac{F(\tau)}{G(\tau)}$, $F(\tau),G(\tau)\in\Lambda_{2k}$, then $f(\tau)\cdot R_a=\frac{F(\tau)\cdot R_a}{G(\tau)\cdot R_a}$. The multipliers τ_p and R_a generate a subring M of the ring of multipliers of the field $\overline{K}$ in itself, which (if one multiplies its tensor by R) is isomorphic to the ring of Hecke operators on Λ_2 and is, together with the latter, a commutative semisimple ring of rank g ([4,5]).

Let q be a prime number, and let the field K be given by the equation $\varphi(x,y)=0$. Then (see [7]) the congruence $\varphi(x,y)\equiv 0 \pmod q$ for almost all q determines the field $K(q)$ of algebraic functions of one variable with a field of constants of q elements, whose genus is equal to the genus of the field K. On the other hand, the field $K(q)$ can be obtained in the following way: the field K is generated by two of its functions $f(\tau)$ and $g(\tau)$, so that $K=R(f,g)$, $\varphi(f,g)=0$. Suppose q does not enter the denominators of the Fourier coefficients of the functions $f(\tau)$ and $g(\tau)$; then for any function $z(\tau)\in K$ there exists such an exponent n that $q^n z(\tau)$ has q-integral Fourier coefficients, not all divisible by q. Replace them by their residues modulo q and associate the resulting formal series with the element $z(\tau)$. Thus a homomorphism of the field K onto the field of algebraic functions of one variable over the field of q elements is defined, which, obviously, coincides with $K(q)$. We shall call admissible those q for which both reductions are admissible, which, moreover, do not enter the denominators of the coefficients of the forms $F_i(\tau)$ and modulo which the $F_i(\tau)$ remain linearly independent. All q, except for a finite number, are admissible. Let $\overline{K}(q)$ be the field obtained from $K(q)$ by algebraic closure of the field of constants, and let $M(q)$ be the image of the ring M under reduction. M and $M(q)$ are semisimple rings (see, respectively, [5,8]). The rank of M is equal to g, the genus of the field K; the

rank of $M(q)$ is also equal to g, for for admissible q the formal expressions $F_i(\tau)\,d\tau$ form a basis of the space of integral differentials of the field $\overline{K}(q)$, and the matrices representing the multipliers of the ring $M(q)$ in this basis are obtained from the matrices representing the corresponding multipliers of the ring M by reducing their elements modulo q. Thus the mapping $M \to M(q)$ is in fact an isomorphism.

Let p be an admissible prime number; then, considering the behavior of the ideal corresponding to the multiplier τ_p in the ring $[\widetilde{K}, \widetilde{K}_0]$ (the tensor product over the field of all algebraic numbers), under reduction modulo p, it is easy to see that

$$\tau_p(p) = R_{p'}(p)\pi^*(p) + \pi(p), \tag{2}$$

where $\pi(p)$ is the Frobenius multiplier; the asterisk denotes application of the Rosati antiautomorphism [6]; $R_{p'}(p)$, $\tau_p(p)$ are the images of $R_{p'}$ and τ_p under reduction modulo p. It is known [9] that the proper numbers of $\pi(p)$ modulo p are equal to $\sqrt{p}$; thus, in view of the indicated isomorphism $M \to M(p)$ and relation (2), it follows that the proper numbers of τ_p, and hence also of $T(p)$ on Λ_2, do not exceed $2\sqrt{p}$ in modulus. From this fact and from the general theory of Hecke operators [4,5], estimate (1) follows without difficulty, where as Q one may take the product of all exceptional prime numbers.

Leningrad Branch
of the V. A. Steklov Mathematical Institute
Academy of Sciences of the USSR

Received
29 V 1961

CITED LITERATURE

[1] M. Eichler, Arch. d. Math., **5**, 355 (1954).
[2] M. Eichler, *Quadratische Formen und orthogonale Gruppen*, Berlin, 1952.
[3] E. Hecke, Abh. Math. Seminar Hamburger Univ., **5**, 199 (1927).
[4] E. Hecke, Math. Ann., **114**, 1 (1937); **6**, 114, 316 (1937).
[5] H. Petersson, Math. Ann., **117**, 39 (1940–1941).
[6] M. Deuring, J. f. reine u. angew. Math., a) **177**, 161 (1937); b) **183**, 25 (1940).
[7] M. Deuring, Math. Zs., **47**, 4, 643 (1942).
[8] A. Weil, *Variétés abéliennes*, Paris, 1948.
[9] A. Weil, *Sur les courbes algébriques*, Paris, 1948.

Note: Figure translations are in progress. See original paper for figures.