JOURNAL OF NUMBER THEORY 9, 61–62 (1977)

Polynomial Sums over Automorphs of a Positive Definite Binary Quadratic Form

RONALD EVANS*

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706 and University of Illinois, Urbana, Illinois 61801

Communicated by P. T. Bateman

Received January 24, 1974

Let $P(X)$ be a homogeneous polynomial in $X = (x, y)$, $Q(X)$ a positive definite integral binary quadratic form, and G the group of integral automorphs of $Q(X)$. Let $A(m) = \{N \in \mathbb{Z} \times \mathbb{Z} : Q(N) = m\}$. It is shown that if $\sum_{N \in A(m)} P(N) = 0$ for each $m = 1, 2, 3,\ldots$, then $\sum_{U \in G} P(UX) \equiv 0$.

Let X denote the vector (x, y), let $P(X)$ denote a homogeneous polynomial $\sum_{j=0}^{n} a_j x^j y^{n-j}$ with complex coefficients, and let $Q(X)$ denote a positive definite integral binary quadratic form $ax^2 + bxy + cy^2$. Define

$$\theta(\tau; P, Q) = \sum_{N \in \mathbb{Z}\times\mathbb{Z}} P(N)\, e^{2\pi i Q(N)\tau}.$$

For each $m \geqslant 1$, let $A(m) = \{N \in \mathbb{Z} \times \mathbb{Z} : Q(N) = m\}$. Note that $\sum_{N \in A(m)} P(N) = 0$ for each $m \geqslant 1$ if and only if $\theta(\tau; P, Q) \equiv 0$. Let G denote the group of integral automorphs (of determinant ± 1) of $Q(X)$. The first result in [1] states that if $P(X)$ is a spherical polynomial with respect to $Q(X)$ and if $\theta(\tau; P, Q) \equiv 0$, then $\sum_{U \in G} P(UX) \equiv 0$. The following theorem shows that this result holds for any homogeneous polynomial $P(X)$, spherical or not.

THEOREM. *If $\sum_{N \in A(m)} P(N) = 0$ for each $m \geqslant 1$, then $\sum_{U \in G} P(UX) \equiv 0$.*

Proof. Let $R(X) = \sum_{U \in G} P(UX)$. Note that $R(X) = R(UX)$ for each $U \in G$. By hypothesis, $\sum_{N \in A(m)} P(N) = 0$, so that $\sum_{N \in A(m)} R(N) = 0$ for each $m \geqslant 1$.

Weber [3] proved that there is an infinite set M consisting of prime

* Current address: Department of Mathematics, University of California at San Diego, La Jolla, California 92093.

ISSN 0022-314X

multiples of $d = \text{g.c.d.}\ (a, b, c)$ such that $Q(X)$ represents each $m \in M$. Moreover, by [2, Theorem 1-6, p. 20], $Q(X)$ represents each $m \in M$ uniquely up to automorphy. Fixing $h_m \in A(m)$, we thus have $A(m) = \{Uh_m : U \in G\}$ for each $m \in M$. Therefore, for each $m \in M$,

$$0 = \sum_{N \in A(m)} R(N) = \sum_{U \in G} R(Uh_m) = \sum_{U \in G} R(h_m) = |\, G \,| \cdot R(h_m),$$

i.e., $R(h_m) = 0$ for each $m \in M$.

If h_m is the vector (x_m, y_m), then x_m and y_m are relatively prime by definition of M. Therefore, the set $B = \{ y_m/x_m : m \in M, x_m \neq 0\}$ is infinite. Write $R(X) = \sum_{i=0}^{n} b_i x^i y^{n-i}$. Each element of B is a zero of the polynomial $\sum_{i=0}^{n} b_i t^{n-i}$, so that all the b_i must vanish. Hence $R(X) \equiv 0$.

References

1. F. Gooding, Jr., Modular forms arising from spherical polynomials and positive definite quadratic forms, *J. Number Theory*, **9** 36–47.
2. W. J. LeVeque, "Topics in Number Theory," Vol. 2, Addison-Wesley, Reading, Mass., 1956.
3. H. Weber, Beweis des Satzes, *Math. Ann.* **20** (1882), 301–329.