ON A HYPOTHESIS ON POINCARÉ SERIES

G. I. Gusev

Let \( F(x_1, \ldots, x_m) \) be a polynomial with integral p-adic coefficients, and let \( N_{\alpha} \) be the number of solutions of the congruence \( F(x_1, \ldots, x_m) \equiv 0 \pmod{p^\alpha} \). A proof is given that the Poincaré series \( \Phi(\alpha) = \sum_{\alpha=0}^{\infty} N_{\alpha} \alpha^\alpha \) is rational for a class of isometrically-equivalent polynomials of \( m \) variables (\( m \geq 2 \)) containing a form of degree \( n \geq 2 \) of two variables.

For a polynomial \( F(x_1, \ldots, x_m) \) with integral p-adic coefficients we denote by \( N_{\alpha} \) the number of solutions of the congruence \( F(x_1, \ldots, x_m) \equiv 0 \pmod{p^\alpha} \) and consider the series \( \Phi(\alpha) = \sum_{\alpha=0}^{\infty} N_{\alpha} \alpha^\alpha \).

There is a hypothesis that the series \( \Phi(\alpha) \), which is called the Fourier series for \( F \) is a rational function ([1], pp. 68–69).

In this paper the author proves that \( \Phi(\alpha) \) is rational for a class of isometrically equivalent polynomials of \( m \) variables, \( m \geq 2 \) containing a form of degree \( n \geq 2 \) of two variables.

Let \( Q_p \) be the field of p-adic numbers, \( Z_p \) be the ring of p-adic integers, \( U_p \) be the group of identity elements of this ring, \( |\ldots| \) is the multiplicative p-adic norm, \( Q_p^m, Z_p^m \) are the \( m \)-th Cartesian powers respectively of \( Q_p \) and \( Z_p \), \( X \) is an arbitrary point of \( Q_p^m \), \( X = (x_1, \ldots, x_m) \); \( \|X\| \) is the norm of the point:

\[
\|X\| = \max_i |x_i|.
\]

Then the normed linear space \( (Q_p^m, |\ldots|) \) over \( Q_p \) is ultrametric if we define the metric \( \rho_m \) in it by the following rule: for and \( X \) and \( Y \) from \( Q_p^m \), \( \rho_m(X, Y) = \|X - Y\| \). Since the ring \( Z_p \) is compact, \( Z_p^m \) is compact.

Definition 1. Let \( X \) and \( Y \) be arbitrary points from \( Z_p^m \), and let \( \sigma \) be a nonnegative integer. We shall say that \( X \) is congruent to \( Y \pmod{p^\sigma} \) and shall write \( X \equiv Y \pmod{p^\sigma} \), if the corresponding coordinates of these points are congruent (mod \( p^\sigma \)).

Definition 2. We shall call the mapping \( \psi : Z_p^m \rightarrow Z_p^m \), for which

\[
\|\psi(X) - \psi(Y)\| = \|X - Y\|
\]

holds, an isometric transformation of \( Z_p^m \).

We shall show that \( \psi \) is a homeomorphism of \( Z_p^m \) onto itself. It is obvious that \( \psi \) is a one-to-one continuous mapping. We now show that \( \psi \) is a mapping onto \( Z_p^m \). In fact, let \( X_0 \) be any point of \( Z_p^m \) and let \( \{X^{(1)}, \ldots, X^{(m)}\} \) be some complete point system of \( Z_p^m \), mutually incongruent (mod \( p^\sigma \), \( \sigma = 1, 2, \ldots \)).

We write \( Y^{(a)} = \psi (X^{(a)}) \). By (1), \( \{Y^{(a)}, \ldots, Y^{(a)}\} \) is also a complete residue class (mod \( p^\sigma \)). Without loss of generality, it may be assumed that for any \( \alpha Y_0 \equiv Y_0 \pmod{p^\alpha} \), and, consequently, \( \lim_{\alpha \to \infty} Y^{(a)} = Y_0 \). By (1), for any \( \alpha \|\psi (X^{(a)}) - \psi (X^{(a+1)})\| = \|X^{(a)} - X^{(a+1)}\| \), i.e., \( \{X^{(a)}\}_{a \to \infty} \) is a Cauchy sequence. Hence, since \( Z_p^m \) is compact, there exists a point \( X_0 \in Z_p^m \), such that \( \lim_{\alpha \to \infty} X^{(a)} = X_0 \). Then \( \psi (X_0) = \lim_{\alpha \to \infty} \psi (X^{(a)}) = \lim_{\alpha \to \infty} Y^{(a)} = Y_0 \), Q.E.D.

Equation (1) is obviously equivalent to the following: for any \( X \) and \( Y \) from \( Z_p^m \), and any integers \( \alpha, \sigma \geq 0 \) such that \( X \equiv Y \pmod{p^\alpha} \), the congruence \( \psi (X) \equiv \psi (Y) \pmod{p^\sigma} \) always holds, and conversely.

An example of an isometric transformation is a transformation of the form

\[ x_i = a_i + \sum_{j=1}^{m} b_{ij} x_j + p^{j_i} (x_i + \ldots + x_m) \quad (1 \leq i \leq m), \tag{2} \]

where \( a_i \in \mathbb{Z}_p \), \( e_i \in \mathbb{U}_p \); \( b_{ij} \in \mathbb{Z}_p \), while \( \det (b_{ij}) \) is a \( p \)-adic identity element \( f_i \); \( g_i \in \mathbb{Z}_p \{X\} \). The property of isometry of this transformation, expressed in terms of congruences, is proved by induction over \( \sigma \).

**Definition 3.** We shall say that two polynomials \( P(X) \) and \( Q(X) \) from the ring \( \mathbb{Z}_p[X] \) are isometrically equivalent; \( P(X) \equiv Q(X) \), if there exists an isometric transformation \( \varphi : \mathbb{Z}_p^m \to \mathbb{Z}_p^m \), such that

\[ P(X) = Q(\varphi(X)) \cdot e(X), \tag{3} \]

where \( e(X) \) is a function defined on \( \mathbb{Z}_p^m \) whose domain is contained in \( \mathbb{U}_p \).

By (3) for any two isometrically equivalent polynomials the Poincaré series coincide. Hence the given hypothesis is equivalent to the hypothesis that the Poincaré series are rational for the class of isometrically equivalent polynomials.

**Theorem 1.** If in the class of is-equivalent polynomials there is a form of degree \( n \geq 2 \) of two variables

\[ \Phi_n(x, y) = \sum_{i=0}^{n} a_i x^i y^{n-i} \]

and if

\[ \Phi_m(t) = \sum_{i=0}^{m} N_a^{(m)} t^i \quad (N_a^{(m)} = N_a^{(m)}(\Phi_n); \ m \gg 2) \tag{4} \]

is the Poincaré series for this class, then (4) is a rational function.

The proof is based on two lemmas.

**Lemma 1.** Let \( I_\delta = p^\delta \cdot \mathbb{Z}_p \), where \( \delta \) is any nonnegative integer, and let \( P_n(x) \) be an arbitrary polynomial with integral \( p \)-adic coefficients not identically equal to zero, \( n = \deg P_n \). We denote by \( N_{\alpha}^{(n)} \) the number of solutions of the congruence \( P_n(x) \equiv 0 \pmod{p^n} \) belonging to \( I_\delta \).

Then there exists a number \( L_\delta = L_\delta (P_n) > 0 \), such that for all \( \alpha > L_\delta \), \( N_{\alpha}^{(n)} = 0 \), if \( P_n(x) \) has no \( p \)-adic roots belonging to \( I_\delta \). If however, \( P_n(x) \) has \( k \)-tuple \( p \)-adic roots \( \mu_i, 1 \leq i \leq n_0 \), belonging to \( I_\delta \), then for all \( \alpha \geq L_\delta \)

\[ N_{\alpha}^{(n)} = \sum_{i=1}^{n_0} C_i^{(p)} p^{\frac{\alpha - \Delta_i}{k_i}}, \tag{5} \]

where \( \Delta_i (1 \leq i \leq n_0) \) are positive integral constants and \( C_i^{(p)} (1 \leq i \leq n_0) \) are nonnegative integral constants.

Proof of the Lemma. The first assertion follows from the compactness of \( \mathbb{Z}_p \). Let us prove the second assertion. Let \( P_n(x) = \sum_{i=1}^{n} a_i x^i \; (a_i \in \mathbb{Z}_p) \). Ex hypothesi \( P_n(x) \neq 0 \). In this case, we introduce the concept of the order of a point of \( \mathbb{Z}_p \) relative to \( P_n(x) \).

**Definition.** We shall say that \( x_0 \in \mathbb{Z}_p \) is of order \( k \) relative to \( P_n(x) \) (we write \( \text{ord}_{P_n} x_0 = k \)) if \( P_n(x) = \ldots = P_n^{(k-1)} (x_0) = 0 \), but \( P_n^{(k)} (x_0) \neq 0 \).

It is obvious that any point \( x_0 \) is of order \( k = k(x_0, P_n) \) subject to the condition: \( 0 \leq k \leq n \). For \( k \geq 1 \) instead of order we may speak of the multiplicity of \( x_0 \) as a root of \( P_n(x) \). We write: \( K = \{ x [x] \equiv \mathbb{Z}_p, \text{ord}_{P_n} x \geq 1 \} \). \( K \) is finite and hence for \( K \neq \emptyset \), there exists a nonnegative integer \( \Delta \) such that for every \( x_0 \in K \) the inequality

\[ \nu_p \left( \frac{1}{k!} P^{(k)}(x_0) \right) \leq \Delta, \tag{6} \]

is satisfied, where \( k_0 = \text{ord}_{P_n} x_0, \nu_p \) is the \( p \)-adic index.

In connection with (6) we take \( I_\delta \) on compacta of the form

\[ K_{L,i}^{(\delta)} = \{ x | \nu_p(x - \mu_i) \gg L, \mu_i = p^{i-1} \} \quad (1 \leq i \leq p^{L-\delta}), \]

where \( L = \max (\Delta + 1, \delta), \{ \theta_i \}_{i=1}^{p^{L-\delta}} \) is some complete residue class \( \pmod{p^{L-\delta}} \).