On an Identity of Hilbert

Yu. V. Nesterenko

ABSTRACT. A simple proof of the polynomial identity used by Hilbert in the solution of the Waring problem is given. The proof is based on the continued fraction expansion of a certain formal hypergeometric series.

KEY WORDS: Waring problem, Hilbert identity, continued fraction, hypergeometric series.

In 1770 J. L. Lagrange proved that each positive integer is the sum of at most four squares of positive integers. In the same year E. Waring conjectured that each positive integer is the sum of at most nine cubes of positive integers, at most 19 biquadratics, and so on.

The first step in the solution of this problem was made in 1859 by Liouville, who proved that any positive integer is the sum of at most 53 biquadratics. In so doing, he used a certain identity for polynomials of four variables. Later, for the same purpose Lucas suggested the simpler identity

\[ 6(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2 = \sum_{i,j} ((x_i + x_j)^4 + (x_i - x_j)^4), \]  

the indices in the sum ranging over all pairs of integers \( i, j \) satisfying the condition \( 1 < i < j < 4 \). Afterwards, by the efforts of many mathematicians, similar results were obtained for \( n = 5, 6, 7, 8, 10 \) (see [1]). At the heart of these proofs were increasingly intricate identities similar to (1). For example, Hurwitz, who proved that each positive integer is the sum of at most 36119 eighth powers of integers [2], used an identity whose right-hand side consists of 184 terms.

In 1909 Hilbert proved [3] that each positive integer is representable as the sum of the \( n \)th powers of positive integers whose number does not exceed a certain bound only determined by the exponent \( n \) and independent of the represented number.

This statement is generally agreed to be the solution of the Waring problem. According to a popular belief, Hilbert’s proof is technically very complicated and hard to understand. In fact, this is not so. Hilbert’s paper culminates a succession of researches, extending and developing preceding ideas in a natural way. The main technical difficulties are concentrated in the proof of Theorem 1 formulated below. The derivation of the Waring conjecture from this theorem is absolutely elementary.

**Theorem 1.** For any integer \( m > 1 \) and \( r > 1 \), there exist positive rational numbers \( b_i \) and integers \( a_{ij} \) such that the equation

\[ (x_1^2 + \cdots + x_r^2)^m = \sum_{j=1}^{M} b_j (a_{1j} x_1 + \cdots + a_{rj} x_r)^{2m} \]

holds identically in the \( r \) variables \( x_1, \ldots, x_r \) with \( M = (2m + 1)^r \).

It should be mentioned that Hilbert proved this theorem for \( r = 5 \) and a smaller value of \( M \). However, the value of \( M \) is of no importance for the solution of the Waring problem in his formulation.

Theorem 1 was stated in Hurwitz’s paper [2] as a conjecture and was used there to prove that the validity of the Waring problem for the exponent \( m \) implies its validity for the exponent \( 2m \). Theorem 1 was first proved by Hilbert [3] by using multiple integrals over a multidimensional ball. Simultaneously with Hilbert’s paper, Hausdorff published the work [4], in which he gave a different proof of the theorem that
made use of multiple improper integrals and the orthogonal Hermite polynomials. It turned out later that Hausdorff’s proof can be worked out without using integrals. In the subsequent three years Stridsberg [5], Hurwitz [6], Remak [7], and Frobenius [8] found an elementary version of Hausdorff’s arguments. In this paper we give another elementary proof of Theorem 1. In essence, it is also a recast of Hausdorff’s proof.

Let us define a sequence of integers $c_k$ by setting

$$c_{2j} = \frac{(2j)!}{j!}, \quad c_{2j+1} = 0, \quad j \geq 0.$$ 

Suppose that for certain positive integers $n$ and $m$ the real numbers $\alpha_h, \beta_h, h = 1, \ldots, n$, satisfy the conditions

$$\sum_{h=1}^{n} \beta_h \alpha_h^k = c_k, \quad k = 0, 1, \ldots, 2m, \quad \beta_h > 0. \quad (3)$$

Then the equations

$$\sum_{h=1}^{n} \cdots \sum_{h_r=1}^{n} \beta_{h_1} \cdots \beta_{h_r} (\alpha_{h_1} x_1 + \cdots + \alpha_{h_r} x_r)^{2m}$$

$$= \sum_{h_1=1}^{n} \cdots \sum_{h_r=1}^{n} \sum_{k_1+\cdots+k_r=2m} \frac{(2m)!}{k_1! \cdots k_r!} \beta_{h_1} \cdots \beta_{h_r} \alpha_{h_1}^k \cdots \alpha_{h_r}^k x_1^{k_1} \cdots x_r^{k_r}$$

$$= \sum_{k_1+\cdots+k_r=2m} \frac{(2m)!}{k_1! \cdots k_r!} c_{k_1} \cdots c_{k_r} x_1^{k_1} \cdots x_r^{k_r}$$

$$= \frac{(2m)!}{m!} \sum_{j_1+\cdots+j_r=m} \frac{(m)!}{j_1! \cdots j_r!} x_1^{2j_1} \cdots x_r^{2j_r} = \frac{(2m)!}{m!} (x_1^2 + \cdots + x_r^2)^m \quad (4)$$

hold identically in the variables $x_1, \ldots, x_r$. Thus, Theorem 1 will be proved if we establish that for a certain $n$ the system of conditions (3) in the unknown $\alpha_h, \beta_h$ is solvable in rational numbers.

Set the parameter $n$ in (3), (4) to be equal to $2m+1$. Then to prove the theorem it will suffice to show that there exist real numbers $\beta_k$ and distinct real numbers $\alpha_h$ satisfying conditions (3). Indeed, for fixed distinct $\alpha_h$ and $n = 2m + 1$, equations (3) define the numbers $\beta_k$ uniquely. Moreover, the numbers $\beta_k$ depend on the $\alpha_h$ continuously. If we choose the rational numbers $\alpha_h$ close enough to $\alpha_h$ and define the corresponding numbers $\beta_k$ for them by means of equations (3), then the numbers $\beta_k$ will also be close to the numbers $\beta_k$. Then the rational numbers $\alpha_k', \beta_k'$ will satisfy all the conditions (3), which implies the validity of Theorem 1.

Let us define the formal series $f_n(x)$ as follows:

$$f_n(x) = 2^n \sum_{k=0}^{\infty} \frac{(2k+n)!}{k!} x^{-2k-n-1}, \quad n \geq 0.$$ 

Then

$$f_0(x) = \sum_{k=0}^{\infty} c_k x^{-k-1}. \quad (5)$$

**Lemma 1.** We have the following relations:

$$f_1(x) = xf_0(x) - 1, \quad (6)$$

$$f_{n+1}(x) = xf_n(x) - 2nf_{n-1}(x), \quad n \geq 1. \quad (7)$$