Additive Number Theory Seminar: Waring's Problem in General

Robert Baxter
Columbia University

Spring 2024

1 Introduction

The goal is to explore Waring's Problem in general, which corresponds to chapter 3 of the textbook. Previously, we've explored Waring's problem in terms of squares and cubes. Today, we're taking a more general approach and prove the Hilbert-Waring problem. The problem we aim to solve is that g(k) is finite for every positive integer k. We're first going to look at polynomial identities and relate them to Waring's problem. Then we're going to look more into Hilbert's identity. To wrap up, we're going to full circle and prove Waring's problem by induction that says there's a finite constant g(k) that every positive integer can be written as a sum of g(k) kth powers.

2 Polynomial Identities

Let's dive into the realm of polynomial identities. These mathematical expressions are incredibly powerful—they hold true for any value we assign to their variables. An example of one of the most common polynomial identities is the difference of squares. This shows us how complex expressions can be broken down into more manageable parts. But in our case, we're going to look at their polynomial identities that help to solve harder problems like Waring's problem. The following three identities are of the notation of:

$$(x_1 \pm x_2 \pm \cdots \pm x_n)^k = \sum_{\epsilon_2,\ldots,\epsilon_n=\pm 1} (x_1 + \epsilon_2 x_2 + \cdots + \epsilon_n x_n)^k.$$

2.1 Theorem 2.1 (Liouville)

$$\left(x_1^2+x_2^2+x_3^2+x_4^2\right)^2=\frac{1}{6}\sum_{1\le i<j\le 4}(x_i+x_j)^4+\frac{1}{6}\sum_{1\le i<j\le 4}(x_i-x_j)^4$$

is a polynomial identity, and every nonnegative integer is the sum of 53 fourth powers,

Let n be any nonnegative integer. By the division algorithm, n can be written in the form $n = 6q + r$, where $q \geq 0$ and $0 \leq r < 6$. By Lagrange's theorem, the nonnegative integer q can be expressed as a sum of four squares, say $q = a_1^2 + a_2^2 + a_3^2 + a_4^2$. Therefore, we have:

$$6q = 6a_1^2 + 6a_2^2 + 6a_3^2 + 6a_4^2$$

Since each term $6a_i^2$ is a square, and since squaring a square yields a fourth power, $6q$ is the sum of 48 fourth powers (12 fourth powers from each a_i).

For the remainder r, which is less than 6, we can write r as the sum of at most 5 fourth powers, because r can be 0, 1, 2, 3, 4, or 5, and each of these numbers can be expressed as a sum of fourth powers of 0 or 1.

Combining these, we find that any nonnegative integer n can be written as:

$$n = 6q + r$$

which is the sum of 53 fourth powers (48 from $6q$ and up to 5 from r).

$$g(4) \leq 53.$$

2.2 Theorem 2.2 (Fleck)

$$\left(x_1^2+x_2^2+x_3^2+x_4^2\right)^3=\frac{1}{60}\sum_{1\le i<j<k\le 4}(x_i\pm x_j\pm x_k)^6+\frac{1}{30}\sum_{1\le i<j\le 4}(x_i\pm x_j)^6+\frac{3}{5}\sum_{1\le i\le 4}x_i^6$$

is a polynomial identity, and every nonnegative integer is the sum of a bounded number of sixth powers.

2.3 Theorem 2.3 (Hurwitz)

$$\left(x_1^2+x_2^2+x_3^2+x_4^2\right)^4=\frac{1}{840}(x_1+x_2+x_3+x_4)^8+\frac{1}{5040}\sum_{1\le i<j<k\le 4}(2x_i\pm x_j\pm x_k)^8$$

$$+\frac{1}{84}\sum_{1\le i<j\le 4}(x_i \pm x_j)^8 + \frac{1}{840}\sum_{1\le i\le 4}(2x_i)^6$$

is a polynomial identity, and every nonnegative integer is the sum of a bounded number of eighth powers.

These equations help us understand how to break down numbers into parts, making it easier to study Waring's problem. They show us that math can find patterns even in very big problems. Next, we'll see how these patterns help us get closer to solving Waring's problem using Hilbert's identity and step-by-step reasoning, known as induction

3 Hilbert's Identity

Theorem 1 (Hilbert's identity)**.** *For every $k \ge 1$ and $r \ge 1$ there exist an integer M and positive rational numbers a_i and integers $b_{i,j}$ for $i = 1, \ldots, M$ and $j = 1, \ldots, r$ such that*

$$(x_1^2 + \cdots + x_r^2)^k = \sum_{i=1}^{M} a_i (b_{i,1}x_1 + \cdots + b_{i,r}x_r)^{2k}. \tag{1}$$

(Lemma 3.9) Let $k \ge 1$. If there exist positive rational numbers $a_1, \ldots, a_M$ such that every sufficiently large integer n can be written in the form

$$n = \sum_{i=1}^{M} a_i y_i^k,$$

where $y_1, \ldots, y_M$ are nonnegative integers, then Waring's problem is true for exponent k.

Proof. Choose n_0 such that every integer $n \ge n_0$ can be represented in the form (3.6). Let q be the least common denominator of the fractions $a_1, \ldots, a_M$. Then qa_i is an integer for $i = 1, \ldots, M$, and qn is a sum of $\sum_{i=1}^{M} qa_i$ nonnegative kth powers for every $n \ge n_0$. Since every integer $N \ge qn_0$ can be written in the form $N = qn + r$, where $n \ge n_0$ and $0 \le r \le q-1$, it follows that N can be written as the sum of $\sum_{i=1}^{M} qa_i + q - 1$ nonnegative kth powers. Clearly, every nonnegative integer $N < qn_0$ can be written as the sum of a bounded number of kth powers, and so Waring's problem holds for k. This completes the proof. □

(Theorem 3.5) *If Waring's problem holds for k, then it holds for $2k$.*
Proof. We use Hilbert's identity (3.5) for k with $r = 4$:

$$(x_1^2 + \ldots + x_4^2)^k = \sum_{i=1}^{M} a_i (b_{i,1}x_1 + \ldots + b_{i,4}x_4)^{2k}.$$

Let y be a nonnegative integer. By Lagrange's theorem, there exist nonnegative integers x_1, x_2, x_3, x_4 such that

$$y = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

and so

$$y^k = \sum_{i=1}^{M} a_i z_i^{2k},$$

where

$$z_i = b_{i,1}x_1 + \ldots + b_{i,4}x_4$$

is a nonnegative integer. This means that

$$y^k = \Sigma(2k)$$

for every nonnegative integer y. If Waring's problem is true for k, then every nonnegative integer is the sum of a bounded number of kth powers, and so every nonnegative integer is the sum of a bounded number of numbers of the form $\Sigma(2k)$. By Lemma 3.9, Waring's problem holds for exponent $2k$. This completes the proof.

4 Proof by Induction of Waring's Problem

Theorem 3.6 (Hilbert–Waring) *The set of nonnegative kth powers is a basis of finite order for every positive integer k.*

Proof. This is by induction on k. The case $k = 1$ is clear, and the case $k = 2$ is Theorem 1.1 (Lagrange's theorem). Let $k \geq 3$, and suppose that the set of ℓth powers is a basis of finite order for every $\ell < k$. By Theorem 3.5, the set of (2ℓ)-th powers is a basis of finite order for $\ell = 1, 2, \ldots, k-1$. Therefore, there exists an integer r such that, for every nonnegative integer n and for $\ell = 1, \ldots, k-1$, the equation

$$n = x_1^{2\ell} + \cdots + x_r^{2\ell}$$

is solvable in nonnegative integers $x_{1,\ell}, \ldots, x_{r,\ell}$. (For example, we could let $r = \max\{g(2\ell) : \ell = 1, 2, \ldots, k-1\}$.)

Let $T \geq 2$. Choose integers $C_1, \ldots, C_{k-1}$ such that

$$0 \leq C_\ell < T \quad \text{for } \ell = 1, \ldots, k-1.$$

There exist nonnegative integers $x_{j,\ell}$ for $j = 1, \ldots, r$ and $\ell = 1, \ldots, k-1$ such that

$$x_1^{2\ell} + \cdots + x_r^{2\ell} = C_{k-\ell}. \tag{3.10}$$

Then

$$x_{j,\ell}^2 \leq \sum_{j=1}^{r} x_{j,\ell}^{2i} \leq C_{k-\ell} < T$$

for $j = 1, \ldots, r$, $\ell = 1, \ldots, k-1$, and $i = 1, \ldots, \ell$. By Lemma 3.10, there exist positive integers $B_{i,\ell}$ depending only on k and ℓ such that

$$x_{j,\ell}^{2\ell} T^{k-\ell} + \sum_{i=0}^{\ell-1} B_{i,\ell} x_{j,\ell}^{2i} T^{k-i} = \sum(2k) = \sum(k). \tag{3.11}$$

Summing (3.11) for $j = 1, \ldots, r$ and using (3.10), we obtain

$$\begin{aligned}
& C_{k-\ell} T^{k-\ell} + \sum_{i=0}^{\ell-1} B_{i,\ell} T^{k-i} \sum_{j=1}^{r} x_{j,\ell}^{2i} \\
&= C_{k-\ell} T^{k-\ell} + T^{k-\ell+1} \sum_{i=0}^{\ell-1} B_{i,\ell} T^{\ell-1-i} \sum_{j=1}^{r} x_{j,\ell}^{2i} \\
&= C_{k-\ell} T^{k-\ell} + D_{k-\ell+1} T^{k-\ell+1} \\
&= \sum(k).
\end{aligned}$$

In this way, every choice of a $(k-1)$-tuple $(C_1, \ldots, C_{k-1})$ of integers in $\{0, 1, \ldots, T-1\}$ determines another $(k-1)$-tuple $(E_1, \ldots, E_{k-1})$ of integers in $\{0, 1, \ldots, T-1\}$. We shall prove that this map of $(k-1)$-tuples is bijective.

It suffices to prove it is surjective. Let $(E_1, \ldots, E_{k-1})$ be a $(k-1)$-tuple of integers in $\{0, 1, \ldots, T-1\}$. There is a simple algorithm that generates integers $C_1, C_2, \ldots, C_{k-1} \in \{0, 1, \ldots, T-1\}$ such that (3.12) is satisfied for some nonnegative integer $E_k < E^*$. Let $C_1 = E_1$ and $I_2 = 0$. Since $D_1 = 0$, we have

$$(C_1 + D_1)T = E_1 T + I_2 T^2.$$

The integer C_1 determines the integer D_2. Choose $C_2 \in \{0, 1, \ldots, T-1\}$ such that

$$C_2 + D_2 + I_2 \equiv E_2 \pmod{T}.$$

There exists a unique integer $C_j \in \{0, 1, \ldots, T-1\}$ such that

$$C_j + D_j + I_j \equiv E_j \pmod{T}.$$

Then

$$C_j + D_j + I_j = E_j + I_{j+1} T$$

for some integer I_{j+1}, and

$$\sum_{\ell=1}^{j} (C_\ell + D_\ell) T^\ell = \sum_{\ell=1}^{j} E_\ell T^\ell + I_{j+1} T^{j+1}.$$

It follows by induction that this procedure generates a unique sequence of integers $C_1, C_2, \ldots, C_{k-1} \in \{0, 1, \ldots, T-1\}$ such that

$$\sum_{\ell=1}^{k-1} (C_\ell + D_\ell) T^\ell = \sum_{\ell=1}^{k-1} E_\ell T^\ell + I_k T^k.$$

Then $n = \sum(k)$ if $T \geq T_1$ and

$$5E^* T^k \leq n < 5E^* (T+1)^k. \tag{3.17}$$

Since every integer $n \geq 5E^* T_1^k$ satisfies inequality (3.17) for some $T \geq T_1$, we have

$$n = \sum(k) \quad \text{for all } n \geq 5E^* T_1^k.$$

It follows from Lemma 3.9 that Waring's problem holds for exponent k. This completes the proof of the Hilbert–Waring theorem.