Linnik's Proof of the Waring–Hilbert Theorem

Thomas Johansson

Bachelor's thesis
2016

Populärvetenskaplig sammanfattning

Ett sedan antiken känt matematiskt problem är frågan om vilket naturligt tal som helst går att skriva om som summan av fyra kvadrater. Det vill säga, finns det, för vilket n som helst, fyra heltal a_1, a_2, a_3, a_4 så att

$$a_1^2 + a_2^2 + a_3^2 + a_4^2 = n?$$

Att så faktiskt är fallet bevisades av Joseph Louis Lagrange år 1770. Ett bevis av satsen ges också i denna uppsats. Metoden som används här är att först visa att om satsen gäller för alla primtal p_1, p_2, p_3 och så vidare, så gäller den också för alla sammansatta tal $n = p_1 \dots p_m$ för något m. Sedan visas att påståendet gäller för alla primtal. Och därmed är satsen bevisad.

Nästa fråga att ställa sig är förstås om det finns en liknande regel för kuber. Alltså, är det så att, för vilket naturligt tal n som helst, det finns h heltal $a_1, a_2, \dots, a_h$ så att

$$a_1^3 + a_2^3 + \cdots + a_h^3 = n?$$

Svaret på denna fråga är också jakande. Det visar sig nämligen att högst nio kuber behövs för att skriva vilket naturligt tal som helst. Naturligtvis kan vi fortsätta, och fråga oss om alla naturliga tal kan skrivas som summan av ett visst antal fjärdepotenser, om de kan skrivas som ett visst antal femtepotenser och så vidare. För den intresserade påpekar vi att nitton fjärdepotenser behövs för att skriva vilket naturligt tal som helst, och att trettiosju femtepotenser behövs för samma syfte. Men i den här uppsatsen är vi inte primärt intresserade av att finna h för en mängd olika potenser. Här ska vi försöka finna en mer generell regel.

Samma år som Lagrange visade att alla naturliga tal kan skrivas som summan av fyra kvadrater, frågade sig den brittiske matematikern Edward Waring om det för ett givet k alltid finns ett h så att det, för varje naturligt tal n alltid finns heltal $a_1, a_2, \dots, a_h$ så att

$$a_1^k + a_2^k + \cdots + a_h^k = n.$$

Frågan är alltså om det alltid, för vilken potens k vi än väljer, bara behövs ett fixt antal k-potenser för att skriva vilket tal som helst. Naturligtvis kommer detta antal att växa med k, men vad Waring förmodade, var att det för ett givet k ändå aldrig skulle bli oändligt stort. Denna förmodan bevisades av tysken David Hilbert 1909. Därför kallas satsen Waring–Hilberts sats. Med tiden har dock andra bevis utarbetats. Till exempel upptäckte ryssen Yuri Linnik år 1943 ett bevis som på ett enklare sätt visade Hilbert–Warings sats. Detta bevis har senare gjorts om och slipats på av flera matematiker runtom i världen. Och det är detta bevis som återges i denna uppsats.

Abstract

In number theory, Waring–Hilbert's theorem guarantees that for each k there is an integer $h \geq 0$ so that, for every non-negative integer n there are non-negative integers $a_1, a_2, \ldots, a_k$ such that

$$a_1^k + a_2^k + \cdots + a_h^k = n.$$

In this thesis the problem will first be proved in the specific case where $k = 2$. Then the proof of the general case due to Yuri Linnik will be given. The notion of Shnirelman density will be introduced. Although the approach for proving Waring–Hilbert's theorem is elementary, several methods from various fields of mathematics will be used. Instances of the Riemann zeta function will be used in order to show that h is finite. The lasts steps in the argument will be carried out with the aid of Fourier series.

Contents

1 Introduction

A question which may arise for any person interested in mathematics is whether any primitive number can be represented as a finite number of squares. In 1770 this was proved by Joseph Louis Lagrange. Actually, he showed that for each positive integer n there are non-negative integers a_1, a_2, a_3, a_4 such that

$$a_1^2 + a_2^2 + a_3^2 + a_4^2 = n.$$

Next, you may ask whether there is a finite number of cubes with which you may represent any positive number, and a finite number of 4th-powers, and 5th-powers and so on. For the record, nine cubes are sufficient for representing any non-negative integer n, and nineteen 4th-powers or thirty-seven 5th-powers suffice for the same task. However, determining how many kth-powers we need for representing any non-negative integer for different k is not what we shall do here. For the same year that Lagrange proved his theorem, Edward Waring[8] made an even bolder assertion. He claimed that, for any positive integer k, there is a finite integer h such that every non-negative integer n may be represented as

$$a_1^k + a_2^k + \cdots + a_h^k = n,$$

where $a_1, a_2, \ldots, a_h$ are non-negative integers. That is, for any k considered, there is a finite h such that every n may be generated. Finding a proof of this assertion is referred to as Waring's problem. Since it was first solved by David Hilbert in 1909[2], the theorem is called the Waring–Hilbert theorem. Many different proofs of the theorem have been proposed. For instance, Hardy and Littlewood[1] may have created the most powerful method for finding the value h for specific k[7]. Here, I shall focus on the the proof first suggested by Yuri Linnik[5] in 1943, which has been further developed by Hua Loo Keng[3] and most recently by Tim Jameson[4]. In this bachelor's thesis I shall generally follow the latter's presentation of the proof.

In section 2 I shall prove Waring's problem in the case $k = 2$. This proof I owe to Melvyn Nathanson[6]. In section 3 I turn to the general assertion. I define and discuss Shnirelman density, which will be crucial later on. The content in that section as well I owe to Nathanson. In section 4 I sketch Linnik's proof of Hilbert–Waring's theorem in order to give an idea of how the theorem will be proved. However, it will be clear that some steps remain to be established. This will be done in section 5. There, I shall complete the proof as it has once been shown by Jameson.

But, before starting, I shall introduce some of the notations I shall use in the thesis.

Definition 1.1 Let a and b be integers, not both zero. Say that there is a positive integer c such that $c \mid a$ and $c \mid b$. Now, if any d such that $d \mid a$ and $d \mid b$ is less than or equal to c, then c is said to be *the greatest common divisor* of a and b, denoted $\gcd(a, b)$.

Definition 1.2 Let a and b be two non-zero integers. Say that there is a positive integer m such that $a \mid m$ and $b \mid m$. Now, if any positive integer n such that $a \mid n$ and $b \mid n$ is greater than or equal to m, then m is said to be *the least common multiple* of a and b, denoted $\operatorname{lcm}(a, b)$.

Definition 1.3 Let a and b be integers. They are said to be *congruent* modulo p if $a - b = kn$ for some integer k. We then write

$$a \equiv b \pmod{p}.$$

Equivalently, upon division by n, a has the remainder b. If a and b are not congruent they are *incongruent*.

Definition 1.4 Let A be a finite set. Then the *cardinality* of A, denoted $|A|$, is the number of elements in A.

Definition 1.5 Say that f and g are functions which depend on x. If there is a c which does not depend on x such that $f(x) \leq cg(x)$ we write

$$f(x) \ll g(x).$$

If c depends on another variable y independent of x, we write

$$f(x) \ll_y g(x).$$

2 Waring's Problem for Squares

Theorem 2.1 Every non-negative integer n may be represented as a sum of four squares.

Proof Assume the integers x and y may be represented as sums of four squares each, that is $x = \sum_{i=1}^{4} x_i^2$ and $y = \sum_{i=1}^{4} y_i^2$. Then, conveniently enough,

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2 \tag{1}$$

where

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 &= x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3 \\ z_3 &= x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2 \\ z_4 &= x_1y_4 - x_4y_1 - x_2y_3 + x_3y_2. \end{aligned} \tag{2}$$

That is, any z with factors x and y which are sums of four squares is the sum of four squares. Hence, we only need show the conclusion for 1 and primes, and the other integers will follow. Now, we know that $1 = 1^2 + 0^2 + 0^2 + 0^2$ and that $2 = 1^2 + 1^2 + 0^2 + 0^2$. Hence, we consider odd primes only.

We note that the set of squares

$$\left\{a^2 \mid a = 0, 1, \ldots, (p-1)/2\right\}$$

consists of $(p+1)/2$ mutually incongruent integers modulo p. If two such squares were congruent, say $a_1^2 \equiv a_2^2 \pmod{p}$, then $a_1^2 - a_2^2 \equiv 0 \pmod{p}$ and $(a_1 + a_2)(a_1 - a_2) \equiv 0 \pmod{p}$. Either the first or the second factor must then be congruent to 0 modulo p. The first one cannot be, for $0 < a_1 + a_2 < p - 1 < p$. The same goes for the second one, for a_1 and a_2 are incongruent modulo p by assumption. It follows that the set

$$\left\{-b^2 - 1 \mid b = 0, 1, \ldots, (p-1)/2\right\}$$

consists of $(p+1)/2$ mutually incongruent integers modulo p as well.

Now, since there are only p residues modulo p, there must be a pair $\left\{a^2, -b^2 - 1\right\}$ which is congruent. That is, $a^2 \equiv -b^2 - 1 \pmod{p}$. Or, equivalently, $a^2 + b^2 + 1 \equiv 0 \pmod{p}$. Let

$$a^2 + b^2 + 1 = a^2 + b^2 + 1^2 + 0^2 = np.$$

What we shall now establish is that $1 \leq n < p$. In order to do so, we see that

$$p \leq np = a^2 + b^2 + 1^2 + 0^2 \leq 2\left(\frac{p-1}{2}\right)^2 + 1 < \frac{p^2}{2} + 1 < p^2.$$

Since $np < p^2$, we obtain $1 \leq n < p$. Now, let m be the least integer such that $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ and $1 \leq m \leq n < p$. The final upshot in the proof will be to show, by reductio ad absurdum, that $m = 1$. Hence, we suppose the opposite, $1 < m < p$. Then there are integers y_1, y_2, y_3 and y_4 such that $y_i \equiv x_i \pmod{m}$, with $-m/2 < y_i \leq m/2$. For these y_i,

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \pmod{m}.$$

This means that there is an r for which $mr = y_1^2 + y_2^2 + y_3^2 + y_4^2$. We shall now establish that $1 \leq r < m$ through three steps.

First, we note that $r \leq m$ since

$$mr = y_1^2 + y_2^2 + y_3^2 + y_4^2 \leq 4(m/2)^2 = m^2.$$

Second, we show that $r \neq m$. Suppose $r = m$. Then $y_i = m/2$ for all i, and $x_i \equiv m/2 \pmod{m}$. Hence, for some k,

$$x_i^2 = (mk + m/2)^2 = m^2(k^2 + k + 1/4) \equiv m^2/4 = (m/2)^2 \pmod{m^2}.$$

This means that

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 4(m/2)^2 = m^2 \equiv 0 \pmod{m^2}$$

which implies that $m \mid p$. But this is impossible since p is prime and $1 < m < p$. This contradiction implies that $r < m$.

Third, we establish that $r \neq 0$. If $r = 0$, then $y_i = 0$, for all i, and $x_i^2 \equiv 0 \pmod{m^2}$. This implies that

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m^2}.$$

Again, this is impossible since p is prime and $1 < m < p$. We have arrived at the conclusion that $1 \leq r < m$.

From the identity (1), we see that

$$(mp)(mr) = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2.$$

But we know that $x_i \equiv y_i \pmod{m}$ for all i. Plugging this information into the equations (2) for z_i, we obtain

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ &\equiv x_1x_1 + x_2x_2 + x_3x_3 + x_4x_4 \\ &= mp \\ &\equiv 0 \pmod{m}, \end{aligned}$$

$$\begin{aligned} z_2 &= x_1y_2 - x_2y_1 - x_3y_4 + x_4y_3 \\ &\equiv x_1x_2 - x_2x_1 - x_3x_4 + x_4x_3 \\ &= 0 \pmod{m}, \end{aligned}$$

$$\begin{aligned} z_3 &= x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2 \\ &\equiv x_1x_3 - x_3x_1 + x_2x_4 - x_4x_2 \\ &= 0 \pmod{m} \end{aligned}$$

and

$$\begin{aligned} z_4 &= x_1y_4 - x_4y_1 - x_2y_3 + x_3y_2 \\ &\equiv x_1x_4 - x_4x_1 - x_2x_3 + x_3x_2 \\ &= 0 \pmod{m}. \end{aligned}$$

That is, $m \mid z_i$ for all i. Hence, there are integers w_i such that $w_i = z_i/m$ and

$$rp = w_1^2 + w_2^2 + w_3^2 + w_4^2,$$

which shows that m is not the least positive integer such that mp is the sum of four squares. Hence, the assumption that $1 < m < p$ is contradicted. Thus, $m = 1$ and the conclusion follows. ■

We have thus seen that every positive integer n may be represented as the sum of four squares, that is $n = \sum_{i=1}^{4} a_i^2$ where a_i are non-negative integers. It has been shown that every positive integer may be represented by nine cubes, that is $n = \sum_{i=1}^{9} a_i^3$. The question arises whether there always is a number $h \geq 1$ of k-powers which may represent every non-negative integer n, that is $n = \sum_{i=1}^{h} a_i^k$. This is the question we shall investigate in the remaining part of this thesis.

3 Shnirelman Density

Definition 3.1 Let A be a set of integers, and let $A(n)$ denote the number of positive integers in A not exceeding n, that is,

$$A(n) = \sum_{\substack{a \in A \\ 1 \leq a \leq n}} 1.$$

The *Shnirelman density* of A, denoted $\sigma(A)$, is defined by

$$\sigma(A) = \inf_{n=1,2,3,\ldots} \frac{A(n)}{n}.$$

For $n > 0$ we have

$$0 \leq A(n) \leq n$$

and hence

$$0 \leq \frac{A(n)}{n} \leq 1.$$

Definition 3.2 Let A and B be sets of integers. Then the *sumset* $A+B$ is the set of integers on the form $a + b$, where $a \in A$ and $b \in B$. We denote the sumset of h identical sets A

$$hA = A + \cdots + A.$$

This set consists of all integers of the form $a_1 + \cdots + a_h$ where each a_i belongs to A. If hA contains every non-negative integer, the set A is called a *basis of order* h. If A is a basis of order $h \geq 1$, A is said to be a *basis of finite order*.

Lemma 3.3 Let A and B be sets of integers such that $0 \in A$ and $0 \in B$. If $n \geq 0$ and $A(n) + B(n) \geq n$, then $n \in A + B$.

Proof If $n \in A$, then $n = n + 0 \in A + B$, since $0 \in B$. Similarly, if $n \in B$, then $n = 0 + n \in A + B$, since $0 \in A$.

Hence, we may suppose that $n \notin A$ and that $n \notin B$. Define sets A' and B' such that

$$A' = \{n - a \mid a \in A, 1 \leq a \leq n - 1\}$$

and

$$B' = \{b \mid b \in B, 1 \leq b \leq n - 1\}.$$

We see that $|A'| = A(n)$ and that $|B'| = B(n)$. Hence,

$$|A'| + |B'| = A(n) + B(n) \geq n.$$

We also see that

$$A' \cup B' \subseteq [1, n - 1].$$

This, along with the conclusion that $|A'| + |B'| \geq n$, means that

$$A' \cap B' \neq \varnothing.$$

It follows that there is an element in A', say $n - a$, which is equal to an element in B', say b. Since $n - a = b$, we see that $n = a + b \in A + B$. ■

Lemma 3.4 Let A and B be sets of integers such that $0 \in A$ and $0 \in B$. If $\sigma(A) + \sigma(B) \geq 1$, then $n \in A + B$ for every non-negative integer n.

Proof If $n \geq 0$, then

$$A(n) + B(n) \geq \sigma(A)n + \sigma(B)n = (\sigma(A) + \sigma(B))n \geq n.$$

Hence, $A(n) + B(n) \geq n$, and Lemma 3.3 implies the result. ■

Corollary 3.5 Let A be a set of integers such that $0 \in A$ and $\sigma(A) \geq 1/2$. Then A is a basis of order 2.

Proof Our approach is the same as in the proof of Lemma 3.4.

$$A(n) + A(n) \geq (\sigma(A) + \sigma(A))n \geq n.$$

Since $A(n) + A(n) \geq n$ Lemma 3.3 implies that $n \in 2A$ for all n. Hence, by definition, A is a basis of order 2. ■

Lemma 3.6 Let A and B be sets of integers such that $0 \in A$ and $0 \in B$. Then

$$\sigma(A + B) \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B).$$

Proof The strategy is to find three distinct types of integers (i), (ii), (iii) which belong to the sumset $A + B$ and are contained in the interval $[0, n]$. Added together, these types of integers will grant the result.

(i) The first type of integers consists of the elements of A. This is permitted, for let $n \geq 1$, let $a_0 = 0$ and let

$$1 \leq a_1 < a_2 < \cdots < a_k \leq n$$

be the $k = A(n)$ positive elements of A not exceeding n. We know that $0 \in B$, so

$$a_i = a_i + 0 \in A + B$$

for all $i = 1, 2, \ldots, k$. This is the first type of integers contained in $A + B$.

(ii) The second type of integers in $A + B$ consists of all numbers $a + b$ greater than a_i but less than a_{i+1} for $i = 0, 1, \ldots, k - 1$. Let

$$1 \leq b_1 < b_2 < \cdots < b_{r_i} \leq a_{i+1} - a_i - 1$$

be the $r_i = B(a_{i+1} - a_i - 1)$ positive integers in B less than $a_{i+1} - a_i$. Then

$$a_i < a_i + b_1 < a_i + b_2 < \cdots < a_i + b_{r_i} < a_{i+1}$$

and

$$a_i + b_j \in A + B$$

for $j = 1, 2, \ldots, r_i$. It is clear that the elements described in (ii) are distinct from those described in (i).

(iii) The third type of integers in $A + B$ consists of all numbers $a + b$ which exceeds the last element a_k in (i). Let

$$1 < b_1 < b_2 < \cdots < b_{r_k} \leq n - a_k$$

be the $r_k = B(n - a_k)$ positive elements of B not exceeding $n - a_k$. Then

$$a_k < a_k + b_1 < a_k + b_2 < \cdots < a_k + b_{r_k} \leq n$$

and

$$a_k + b_j \in A + B$$

for $j = 1, 2, \ldots, r_k$. It is clear that the elements in (iii) are distinct from those in (ii) or (i).

Added together, these three types of integers grant

$$\begin{aligned}
(A + B)(n) &\geq A(n) + \sum_{i=0}^{k-1} B(a_{i+1} - a_i - 1) + B(n - a_k) \\
&\geq A(n) + \sigma(B) \sum_{i=0}^{k-1} (a_{i+1} - a_i - 1) + \sigma(B)(n - a_k) \\
&= A(n) + \sigma(B) \sum_{i=0}^{k-1} (a_{i+1} - a_i) - \sigma(B)k + \sigma(B)n - \sigma(B)a_k. \qquad (3)
\end{aligned}$$

Now, since

$$\sum_{i=0}^{k-1} (a_{i+1} - a_i) = (a_1 - a_0) + (a_2 - a_1) + \cdots + (a_k - a_{k-1}) = a_k - a_0 = a_k,$$

(3) equals

$$\begin{aligned}
A(n) + \sigma(B)a_k - \sigma(B)k + \sigma(B)n - \sigma(B)a_k &= A(n) - \sigma(B)k + \sigma(B)n \\
&= A(n) - \sigma(B)A(n) + \sigma(B)n \\
&= A(n)(1 - \sigma(B)) + \sigma(B)n \\
&\geq \sigma(A)n(1 - \sigma(B)) + \sigma(B)n \\
&= \sigma(A)n - \sigma(B)\sigma(A)n + \sigma(B)n \\
&= (\sigma(A) + \sigma(B) - \sigma(A)\sigma(B))n.
\end{aligned}$$

Hence,

$$\frac{(A+B)(n)}{n} \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B)$$

and, therefore,

$$\sigma(A+B) \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B) \tag{4}$$

which completes the proof. ■

Lemma 3.7 Let $h \geq 1$ and $A_1, A_2, \ldots, A_h$ be sets of integers such that $0 \in A_i$ for $i = 1, 2, \ldots, h$. Then

$$1 - \sigma(A_1 + A_2 + \cdots + A_h) \leq \prod_{i=1}^{h} (1 - \sigma(A_i)).$$

Proof We prove the lemma by induction. For $h = 1$ the result is obvious. Next, consider the recently acquired result (4). It is equivalent to

$$1 - \sigma(A+B) \leq (1 - \sigma(A))(1 - \sigma(B))$$

which validates the result for $h = 2$. Hence we let $h \geq 3$ and assume that the lemma holds for $h - 1$. Let B be the sumset $A_2 + A_3 + \cdots + A_h$. The induction hypothesis gives

$$1 - \sigma(B) = 1 - \sigma(A_2 + A_3 + \cdots + A_h) \leq \prod_{i=2}^{h} (1 - \sigma(A_i)).$$

Therefore, as we have shown in the case $h = 2$,

$$\begin{aligned} 1 - \sigma(A_1 + A_2 + \cdots + A_h) &= 1 - \sigma(A_1 + B) \\ &\leq (1 - \sigma(A_1))(1 - \sigma(B)) \\ &\leq (1 - \sigma(A_1)) \prod_{i=2}^{h} (1 - \sigma(A_i)) \\ &= \prod_{i=1}^{h} (1 - \sigma(A_i)). \blacksquare \end{aligned}$$

Theorem 3.8 Let A be a set of integers such that $0 \in A$ and $\sigma(A) > 0$. Then A is a basis of finite order.

Proof We know that $0 \leq 1 - \sigma(A) < 1$, and so

$$0 \leq (1 - \sigma(A))^h \leq 1/2$$

for some integer h. As we have shown,

$$1 - \sigma(hA) \leq (1 - \sigma(A))^h \leq 1/2$$

and so

$$\sigma(hA) \geq 1/2.$$

Now, Corollary 3.5 implies that the set hA is a basis of order 2. Hence, A is a basis of order $2h$. That is, A is a basis of finite order. ■

4 Approaching the Waring–Hilbert Theorem

Let A' be the set

$$\left\{a^k \mid a = 0, 1, 2, \ldots\right\}.$$

We fix a $k \geq 2$, set $h = 8^{k-1}$ and let A be the sumset hA'. Then we note that A is precisely the set of non-negative integers n for which there is at least one solution such that

$$x_1^k + x_2^k + \cdots + x_h^k = n,$$

where x_i are non-negative integers. We define $r(n)$ to be the number of such solutions for such an n. We note that, for $N \geq 1$,

$$A(N) = \sum_{\substack{r(n)\geq 1 \\ 1\leq n\leq N}} 1.$$

We now consider $r(n)$ for every $0 \leq n \leq N$. We see that

$$\begin{aligned}
\sum_{n=0}^{N} r(n) &= \sum_{\substack{x_1,\ldots,x_h\geq 0 \\ x_1^k+\cdots+x_h^k\leq N}} 1 \\
&\geq \sum_{0\leq x_1,\ldots,x_h\leq (N/h)^{1/k}} 1 \\
&\geq (N/h)^{h/k} \\
&= (1/h^{h/k})N^{h/k}.
\end{aligned}$$

Since $1/h^{h/k}$ depends only on the fixed k,

$$\sum_{n=0}^{N} r(n) \gg_k N^{h/k}. \tag{5}$$

But we can also deduce

$$\begin{aligned}
r(n) &= \sum_{\substack{0\leq x_1,\ldots,x_h\leq n^{1/k} \\ x_1^k+\cdots+x_h^k=n}} 1 \\
&= \sum_{0\leq x_1,\ldots,x_h\leq n^{1/k}} \int_0^1 e^{2\pi i(x_1^k+\cdots+x_h^k-n)\alpha} d\alpha \\
&= \int_0^1 \left(\sum_{0\leq x\leq n^{1/k}} e^{2\pi i x^k\alpha}\right)^h e^{-2\pi i n\alpha} d\alpha \\
&\leq \int_0^1 \left|\sum_{0\leq x\leq n^{1/k}} e^{2\pi i x^k\alpha}\right|^h d\alpha.
\end{aligned}$$

The major difficulty in our mission will be to show that

$$\int_0^1 \left|\sum_{0\leq x\leq n^{1/k}} e^{2\pi i x^k\alpha}\right|^h d\alpha \ll_k n^{h/k-1} \tag{6}$$

When that is done, we receive

$$r(n) \ll_k n^{h/k-1}.$$

We shall now sum the $r(n)$.

$$\begin{aligned}\sum_{n=0}^{N} r(n) &= r(0) + \sum_{n=1}^{N} r(n) \\ &\ll_k 1 + N^{h/k-1} \cdot A(N). \end{aligned} \tag{7}$$

(5) and (7) taken together give the relations

$$0 < N^{h/k} \ll_k \sum_{n=0}^{N} r(n) \ll_k 1 + N^{h/k-1} \cdot A(N),$$

which implies that

$$1 \ll_k N^{-h/k} + \frac{A(N)}{N}.$$

That is, there is a constant c which depends only on k such that

$$1 < c\left(N^{-h/k} + \frac{A(N)}{N}\right).$$

Therefore, there is a finite number $N_0 \geq 1$ such that

$$0 < \frac{1 - cN_0^{-h/k}}{c} < \frac{A(N)}{N},$$

where $N > N_0$. Since N_0 is finite, we reach the conclusion:

Theorem 4.1 The set A has positive Shnirelman density.

This theorem will, with the aid of Theorem 3.8, show that A is a set of finite order, and, moreover, that the set A' is a set of finite order. However, to complete the proof of this theorem we have to establish the inequality (6). That is what we shall do in the next section.

5 Linnik's proof

At the end of this section, we shall show (6) by induction. In order to do so, we need some preliminary lemmas.

Lemma 5.1 Let m_1 and m_2 be integers, not both zero, and let $q(n, m_1, m_2)$ be the number of integer solutions to the equation

$$x_1 m_1 + x_2 m_2 = n \tag{8}$$

when x_1 and x_2 are in the interval $[-N, N]$, that is

$$q(n, m_1, m_2) = \sum_{\substack{x_1, x_2 = -N \\ x_1 m_1 + x_2 m_2 = n}}^{N} 1.$$

If $g = \gcd(m_1, m_2)$ is not a divisor of n there are no solutions to the equation. Hence, we consider the cases when $g \mid n$, so that $m_1 = a_1 g$, $m_2 = a_2 g$ and $n = bg$. Then

$$q(n, m_1, m_2) \leq \frac{2N}{\max(|a_1|, |a_2|)} + 1.$$

Proof Since $m_1 = a_1 g$, $m_2 = a_2 g$ and $n = bg$, the equation (8) becomes

$$x_1 a_1 + x_2 a_2 = b.$$

We note that the diophantine equation $x_1 a_1 + x_2 a_2 = 1$ has a solution $x_1 = \overline{a}_1$ and $x_2 = \overline{a}_2$. Combining these two equations we receive

$$x_1 a_1 + x_2 a_2 = b(\overline{a}_1 a_1 + \overline{a}_2 a_2)$$

which is equivalent to

$$a_1(x_1 - b\overline{a}_1) + a_2(x_2 - b\overline{a}_2) = 0.$$

We see that the general solution is on the form

$$\begin{aligned} x_1 &= b\overline{a}_1 + k a_2 \\ x_2 &= b\overline{a}_2 - k a_1. \end{aligned}$$

There is no harm in assuming $a_1 \geq a_2 \geq 0$, where at least $a_1 > 0$. This implies that

$$q(n, m_1, m_2) = \sum_{\substack{k: \\ -N - b\overline{a}_1 \leq k a_2 \leq N - b\overline{a}_1 \\ -N + b\overline{a}_2 \leq k a_1 \leq N + b\overline{a}_2}} 1.$$

That is, we count the integers in the intersection of two intervals of length $2N/a_1$ and $2N/a_2$. We need only consider the shortest one, that is the one of length $2N/a_1$. Such an interval contains at most $2N/a_1 + 1$ integers. Hence the lemma is proved. ■

We shall now count the total number of solutions x_1, x_2 in $[-N, N]$ when m_1 and m_2 range over $[-M, M] \setminus \{0\}$. The number of these solutions we call $q(n)$, that is

$$q(n) = \sum_{\substack{m_1, m_2 = -M \\ m_1, m_2 \neq 0}}^{M} \sum_{\substack{x_1, x_2 = -N \\ x_1 m_1 + x_2 m_2 = n}}^{N} 1.$$

The next lemma estimates $q(n)$.

Lemma 5.2

$$q(n) \leq \begin{cases} 20MN \sum_{g \mid n} 1/g & \text{if } n \neq 0 \text{ and } N \geq M \\ 20M^2 N & \text{if } n = 0. \end{cases}$$

Proof From Lemma 5.1 we know that

$$\begin{aligned}
q(n) &= \sum_{\substack{m_1,m_2=-M \\ m_1,m_2\neq 0}}^{M} q(n,m_1,m_2) \\
&= 4\sum_{m_1,m_2=1}^{M} q(n,m_1,m_2) \\
&\leq 4\sum_{m_1,m_2=1}^{M}\left(\frac{2N}{\max(|a_1|,|a_2|)}+1\right) \\
&\leq 4M^2+8N\sum_{\substack{g|n \\ g\leq M}}\sum_{\substack{1\leq a_1\leq M/g \\ 0\leq a_2\leq M/g}}\frac{1}{\max(|a_1|,|a_2|)} \\
&= 4M^2+8N\sum_{\substack{g|n \\ g\leq M}}\left(\sum_{1\leq a_1\leq M/g}\sum_{0\leq a_2<a_1}\frac{1}{a_1}+\sum_{1\leq a_2\leq M/g}\sum_{1\leq a_1\leq a_2}\frac{1}{a_2}\right) \\
&= 4M^2+16N\sum_{\substack{g|n \\ g\leq M}}\sum_{1\leq a\leq M/g}1 \\
&\leq 4M^2+16NM\sum_{\substack{g|n \\ g\leq M}}\frac{1}{g}.
\end{aligned}$$

If $n=0$, then the second term equals $16NM\sum_{g=1}^{M}1/g$, and $q(n)\leq 4M^2+16NM^2\leq 20M^2N$. On the other hand, in the case where $n\neq 0$, then the first term is less or equal to $4MN$, since $N\geq M$, and so $q(n)\leq 20MN\sum_{g|n}1/g$. This proves the lemma. ■

Now we shall pay attention to some instances of the Riemann zeta function. For $s>1$, the function sums up all $1/p^s$ when p goes from 1 to infinity. That is, the Riemann zeta function is defined by

$$\zeta(s)=\sum_{p=1}^{\infty}\frac{1}{p^s}.$$

For several instances of the Riemann zeta function, its value is known. This will be used in the two following lemmas.

Lemma 5.3

$$\sum_{\substack{a,b=1 \\ \gcd(a,b)=1}}^{\infty}\frac{1}{a^2b^2}=\frac{5}{2}$$

Proof Say that $\gcd(d,e)=g$, $d=ga$ and $e=gb$, so that $\gcd(a,b)=1$. We directly see that

$$\sum_{d,e=1}^{\infty}\frac{1}{d^2e^2}=\left(\sum_{p=1}^{\infty}\frac{1}{p^2}\right)^2.$$

This equals $\pi^4/36$, since it is the square of a known instance of the Riemann zeta function which equals $\pi^2/6$. We also see that

$$\sum_{d,e=1}^{\infty} \frac{1}{d^2e^2} = \sum_{\substack{g,a,b=1 \\ \gcd(a,b)=1}}^{\infty} \frac{1}{g^4a^2b^2} = \sum_{p=1}^{\infty} \frac{1}{p^4} \sum_{\substack{a,b=1 \\ \gcd(a,b)=1}}^{\infty} \frac{1}{a^2b^2},$$

where we recognize another instance of the Riemann zeta function which equals $\pi^4/90$. Hence,

$$\sum_{\substack{a,b=1 \\ \gcd(a,b)=1}}^{\infty} \frac{1}{a^2b^2} = \frac{\left(\sum_{p=1}^{\infty} \frac{1}{p^2}\right)^2}{\sum_{p=1}^{\infty} \frac{1}{p^4}} = \frac{\pi^4/36}{\pi^4/90} = \frac{5}{2}$$

and the lemma is proved. ■

Lemma 5.4 We have

$$\sum_{n \le N} \left(\sum_{d|n} \frac{1}{d} \right)^2 \le \frac{5N}{2} \sum_{p=1}^{\infty} \frac{1}{p^3},$$

where the instance of the Riemann zeta function is known as Apéry's constant. Later on, we shall use that $\sum_{p=1}^{\infty} \frac{1}{p^3} \approx 1.202$.

Proof

$$\begin{aligned}
\sum_{n \le N} \left(\sum_{d|n} \frac{1}{d} \right)^2 &= \sum_{n \le N} \sum_{d,e|n} \frac{1}{de} \\
&= \sum_{d,e \le N} \left(\frac{1}{de} \sum_{\substack{n \le N \\ d,e|n}} 1 \right) \\
&= \sum_{d,e \le N} \left(\frac{1}{de} \sum_{\substack{n \le N \\ n \equiv 0 \pmod{\operatorname{lcm}(d,e)}}} 1 \right) \\
&\le \sum_{d,e \le N} \frac{N}{de \cdot \operatorname{lcm}(d,e)}.
\end{aligned}$$

As in the proof of Lemma 5.3, we say that $\gcd(d,e) = g$, $d = ga$ and $e = gb$, so that $\operatorname{lcm}(d,e) = gab$. Hence

$$\sum_{d,e \le N} \frac{N}{de \cdot \operatorname{lcm}(d,e)} = N \sum_{\substack{g,a,b=1 \\ \gcd(a,b)=1}}^{N} \frac{1}{g^3a^2b^2} \le N \sum_{p=1}^{\infty} \frac{1}{p^3} \sum_{\substack{a,b=1 \\ \gcd(a,b)=1}}^{\infty} \frac{1}{a^2b^2} = \frac{5N}{2} \sum_{p=1}^{\infty} \frac{1}{p^3}$$

and the lemma is proved. ■

Lemma 5.5 Suppose that $N \geq M$. Then

$$\sum_{\substack{m_1,\dots,m_4=-M \\ m_1,\dots,m_4\neq 0 \\ m_1n_1+m_2n_2=m_3n_3+m_4n_4}}^{M} \sum_{n_1,\dots,n_4=-N}^{N} 1 \leq 5250(MN)^3.$$

Proof We have, by Lemma 5.2 and Lemma 5.4, that

$$\begin{aligned}
\sum_{\substack{m_1,\dots,m_4=-M \\ m_1,\dots,m_4\neq 0 \\ m_1n_1+m_2n_2=m_3n_3+m_4n_4}}^{M} \sum_{n_1,\dots,n_4=-N}^{N} 1 &= \sum_{n=-2MN}^{2MN} q(n)^2 \\
&\leq 20^2 \left(M^4N^2 + 2M^2N^2 \sum_{n=1}^{2MN} \left(\sum_{g|n} \frac{1}{g} \right)^2 \right) \\
&\leq 20^2 \left(M^4N^2 + 2M^2N^2 \frac{5 \cdot 2MN}{2} \sum_{p=1}^{\infty} \frac{1}{p^3} \right) \\
&= 20^2 \left(M^4N^2 + 10(MN)^3 \sum_{p=1}^{\infty} \frac{1}{p^3} \right) \\
&\leq 20^2 (MN)^3 \left(1 + 10 \sum_{p=1}^{\infty} \frac{1}{p^3} \right).
\end{aligned}$$

Since $\sum_{p=1}^{\infty} \frac{1}{p^3} \approx 1.202$, we see that $20^2 \left(1 + 10 \sum_{p=1}^{\infty} \frac{1}{p^3}\right) \leq 5250$, which now proves the lemma. ■

Lemma 5.6 Suppose that $N \geq 2M$. Then

$$\sum_{\substack{m_1,\dots,m_4=-M \\ m_1n_1+m_2n_2=m_3n_3+m_4n_4}}^{M} \sum_{n_1,\dots,n_4=-N}^{N} 1 \leq 162N^4 + 5250(MN)^3.$$

Proof Define

$$\begin{aligned}
Q(n) &= \sum_{m_1,m_2=-M}^{M} \sum_{\substack{n_1,n_2=-N \\ m_1n_1+m_2n_2=n}}^{N} 1 \\
&= \sum_{m_1,m_2=-M}^{M} q(n, m_1, m_2) \\
&= q(n,0,0) + 4 \sum_{\substack{1\leq m_1\leq M \\ 0\leq m_2\leq M}} q(n, m_1, m_2).
\end{aligned}$$

Of course, $q(n,0,0) = 0$ when $n \neq 0$. In that case, we obtain the same bound for $Q(n)$ as that for $q(n)$ in Lemma 5.2. In the proof of Lemma 5.2 the $4M^2$ will be replaced by $4M(M+1)$,

but since $M < N$ we still have $4M(M+1) \leq 4MN$. However, when $n = 0$ we see that $q(n,0,0) = (2N+1)^2 \leq 9N^2$. Hence, we have

$$Q(0) \leq 9N^2 + 20M^2N,$$

and hence

$$\begin{aligned} Q(0)^2 &\leq 2(9N^2)^2 + 2(20M^2N)^2 \\ &= 162M^4 + 20^2M^3N^2 \cdot 2M \\ &\leq 162M^4 + 20^2(MN)^3. \end{aligned}$$

Hence, using the working of Lemma 5.5,

$$\sum_{\substack{m_1,\ldots,m_4=-M \\ m_1n_1+m_2n_2=m_3n_3+m_4n_4}}^{M} \sum_{n_1,\ldots,n_4=-N}^{N} 1 = \sum_{n=-2MN}^{2MN} Q(n)^2 \leq 162N^4 + 5250(MN)^3,$$

and the lemma is proved. ■

We are now beginning the proof of the inequality (6). Since we shall prove it by induction, we need to show it for $k = 2$. This is what we shall do now.

Lemma 5.7 Let

$$f(n) = a_2n^2 + a_1n$$

where a_1, a_2 are integers with $|a_1| \leq c_1N$ and $0 < |a_2| \leq c_2$. Then, for $N \geq 1$ and $C = 162(2c_2 + c_1)^4 + 5250(2c_2 + c_1)^3$, we have

$$\int_0^1 \left| \sum_{n=0}^{N} e^{2\pi i f(n)\alpha} \right|^8 d\alpha \leq CN^6.$$

Proof

$$\begin{aligned} \int_0^1 \left| \sum_{n=0}^{N} e^{2\pi i f(n)\alpha} \right|^8 d\alpha &= \int_0^1 \left| \sum_{n=0}^{N} e^{2\pi i f(n)\alpha} \right|^4 \left| \sum_{n=0}^{N} e^{2\pi i f(n)\alpha} \right|^4 d\alpha \\ &= \int_0^1 \left(\sum_{n=0}^{N} e^{2\pi i f(n)\alpha} \right)^4 \left(\sum_{n=0}^{N} e^{-2\pi i f(n)\alpha} \right)^4 d\alpha \\ &= \int_0^1 \sum_{n_1,\ldots,n_8=0}^{N} e^{2\pi i(f(n_1)+\cdots+f(n_4)-f(n_5)-\cdots-f(n_8))\alpha} d\alpha \\ &= \sum_{n_1,\ldots,n_8=0}^{N} \int_0^1 e^{2\pi i(f(n_1)+\cdots+f(n_4)-f(n_5)-\cdots-f(n_8))\alpha} d\alpha \\ &= \sum_{\substack{n_1,\ldots,n_8=0 \\ f(n_1)+\cdots+f(n_4)=f(n_5)+\cdots+f(n_8)}}^{N} 1. \end{aligned} \tag{9}$$

The equation $f(n_1) + \cdots + f(n_4) = f(n_5) + \cdots + f(n_8)$ may be written as

$$\begin{aligned}\sum_{i=1}^{4} (f(n_i) - f(n_{i+4})) &= \sum_{i=1}^{4} \big(a_2(n_i^2 - n_{i+4}^2) + a_1(n_i - n_{i+4})\big) \\ &= \sum_{i=1}^{4} m_i x_i \\ &= 0,\end{aligned}$$

where $m_i = n_i - n_{i+4}$ and $x_i = a_2(n_i + n_{i+4}) + a_1$. We see that $-N \leq m_i \leq N$, while $-N(2c_2 + c_1) \leq x_i \leq N(2c_2 + c_1)$, which, since $c_2 \geq 1$, means that Lemma 5.6 is applicable to the situation. (9) equals

$$\begin{aligned}\sum_{\substack{n_1,\ldots,n_8=0 \\ m_1x_1+\cdots+m_4x_4=0}}^{N} 1 &\leq \sum_{m_1,\ldots,m_4=-N}^{N} \sum_{\substack{x_1,\ldots,x_4=-N(2c_2+c_1) \\ m_1x_1+\cdots+m_4x_4=0}}^{N(2c_2+c_1)} 1 \\ &= \sum_{m_1,\ldots,m_4=-N}^{N} \sum_{\substack{x_1,\ldots,x_4=-N(2c_2+c_1) \\ m_1x_1+m_2x_2=m_3x_3+m_4x_4}}^{N(2c_2+c_1)} 1,\end{aligned}$$

which, according to Lemma 5.6, is less or equal to

$$162N^4(2c_2 + c_1)^4 + 5250N^6(2c_2 + c_1)^3 \leq CN^6$$

and the result follows. ■

In the proof of the crucial theorem we shall apply Hölder's inequality. This will not be proved:

Theorem 5.8 Hölder's inequality states that

$$\sum_{k=1}^{n} |u_k v_k| \leq \left(\sum_{k=1}^{n} |u_k|^p\right)^{1/p} \left(\sum_{k=1}^{n} |v_k|^q\right)^{1/q}$$

for p and q such that $1/p + 1/q = 1$.

We are now ready to prove the inequality (6).

Theorem 5.9 Let $k \geq 2$ and

$$f(n) = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n$$

where $a_1, a_2, \ldots, a_k$ are integers and $a_k \neq 0$. Let $N \geq 1$ and $|a_j| \ll_{k,j} N^{k-j}$. The inequality $\ll_{k,j}$ hence depends on both k and j. That means that there are k different constants which ensure the inequalities. Call these constants $d_1, d_2, \ldots, d_k$. Then

$$\int_0^1 \left|\sum_{n=0}^{N} e^{2\pi i f(n)\alpha}\right|^{8^{k-1}} d\alpha \ll_{k,d_1,d_2,\ldots,d_k} N^{8^{k-1}-k}.$$

For simplicity, we shall from now on omit the suffices in the $\ll_{k,d_1,d_2,\ldots,d_k}$ notation, and be settled with $\ll$.

Proof As mentioned, we shall prove the theorem by induction. Lemma 5.7 establishes that it holds for $k = 2$. We shall assume that it holds for the case $k - 1$. We have

$$\begin{aligned}
\left|\sum_{n=0}^{N} e^{2\pi i f(n)\alpha}\right|^2 &= \left|\sum_{n=0}^{N} e^{2\pi i f(n)\alpha}\right| \left|\sum_{n=0}^{N} e^{2\pi i f(n)\alpha}\right| \\
&= \left(\sum_{n=0}^{N} e^{2\pi i f(n)\alpha}\right)\left(\sum_{n=0}^{N} e^{-2\pi i f(n)\alpha}\right) \\
&= \sum_{n_1,n_2=0}^{N} e^{2\pi i (f(n_1)-f(n_2))\alpha} \\
&= \sum_{n_1=0}^{N} e^{2\pi i (f(n_1)-f(n_1))\alpha} + \sum_{\substack{n_1,n_2=0 \\ n_1\neq n_2}}^{N} e^{2\pi i (f(n_1)-f(n_2))\alpha} \qquad (10) \\
&= N + 1 + \sum_{\substack{n_1,n_2=0 \\ n_1\neq n_2}}^{N} e^{2\pi i (f(n_1)-f(n_2))\alpha} \\
&= N + 1 + \sum_{\substack{h=-N \\ h\neq 0}}^{N} b_h
\end{aligned}$$

where

$$b_h = \sum_{\substack{n_1,n_2=0 \\ n_1-n_2=h}}^{N} e^{2\pi i (f(n_1)-f(n_2))\alpha} = \sum_{n=\max(0,-h)}^{\min(N,N-h)} e^{2\pi i h (g(n,h))\alpha},$$

where

$$\begin{aligned}
g(n,h) &= \frac{1}{h}\left(f(n+h) - f(n)\right) \\
&= \frac{1}{h}\sum_{j=1}^{k} a_j \left((n+h)^j - n^j\right) \\
&= \sum_{j=1}^{k} a_j \sum_{r=0}^{j-1} \binom{j}{r} h^{j-r-1} n^r \\
&= \sum_{r=0}^{k-1} \left(\sum_{j=r+1}^{k} \binom{j}{r} a_j h^{j-r-1}\right) n^r
\end{aligned}$$

is a polynomial of degree $k-1$ in n. We shall show that this sum is sufficiently small. We see that the coefficient of n^{k-1} in $g(n,h)$ is

$$\binom{k}{k-1} a_k h^{k-(k-1)-1} = k a_k \neq 0.$$

We also see that the coefficient of n^r is

$$\sum_{j=r+1}^{k} \binom{j}{r} a_j h^{j-r-1} \ll \sum_{j=r+1}^{k} \binom{j}{r} N^{k-j} N^{j-r-1} \ll N^{k-r-1}.$$

Now we return to the equation (10) and apply Hölder's inequality, Theorem 5.8, to it:

$$\begin{aligned}\left|\sum_{n=0}^{N} e^{2\pi i f(n)\alpha}\right|^2 &= N+1+\sum_{\substack{h=-N\\h\neq 0}}^{N} b_h \\ &\leq |N|+|1|+\left|\sum_{\substack{h=-N\\h\neq 0}}^{N} b_h\right| \\ &\leq (1^p+1^p+1^p)^{1/p}\left(|N|^q+|1|^q+\left|\sum_{\substack{h=-N\\h\neq 0}}^{N} b_h\right|^q\right)^{1/q} \\ &= 3^{1/p}\left(|N|^q+|1|^q+\left|\sum_{\substack{h=-N\\h\neq 0}}^{N} b_h\right|^q\right)^{1/q}.\end{aligned}$$

We choose

$$q = 8^{k-2}$$

and

$$p = \frac{8^{k-2}}{8^{k-2}-1}.$$

This means that $1/p + 1/q = 1$, as demanded by Theorem 5.8. Raising our results to the power 8^{k-2} gives

$$\begin{aligned}\left|\sum_{n=0}^{N} e^{2\pi i f(n)\alpha}\right|^{2\cdot 8^{k-2}} &\ll |N|^{8^{k-2}}+|1|^{8^{k-2}}+\left|\sum_{\substack{h=-N\\h\neq 0}}^{N} b_h\right|^{8^{k-2}} \\ &\ll N^{8^{k-2}}+\left|\sum_{\substack{h=-N\\h\neq 0}}^{N} b_h\right|^{8^{k-2}} \\ &\ll N^{8^{k-2}}+\left(\sum_{\substack{h=-N\\h\neq 0}}^{N} 1\right)^{8^{k-2}-1}\sum_{\substack{h=-N\\h\neq 0}}^{N}|b_h|^{8^{k-2}} \\ &\ll N^{8^{k-2}}+N^{8^{k-2}-1}\sum_{\substack{h=-N\\h\neq 0}}^{N}|b_h|^{8^{k-2}}.\end{aligned}$$

We raise this to a fourth power and integrate over α and receive

$$\int_0^1\left|\sum_{n=0}^{N} e^{2\pi i f(n)\alpha}\right|^{8^{k-1}} d\alpha \ll N^{4\cdot 8^{k-2}}+N^{4\cdot 8^{k-2}-4}\int_0^1\left(\sum_{\substack{h=-N\\h\neq 0}}^{N}|b_h|^{8^{k-2}}\right)^4 d\alpha. \qquad (11)$$

The function b_h has period $1/|h|$. Now $|b_h|^{8^{k-2}}$ has the Fourier series

$$|b_h|^{8^{k-2}} = \sum_{m=-\infty}^{\infty} C_m(h) e^{2\pi i m h \alpha}.$$

This is finite since

$$C_m(h) \neq 0 \Rightarrow m \ll \max_{0 \leq n \leq N} |g(n,h)| \ll N^{k-1}$$

which means that the range for m may be written as $|m| \leq CN^{k-1}$. The coefficients are given by

$$\begin{aligned} C_m(h) &= |h| \int_0^{1/|h|} |b_h(\alpha)|^{8^{k-2}} e^{-2\pi i m |h| \alpha} d\alpha \\ &= |h| \int_0^{1/|h|} \left| \sum_{n=\max(0,-h)}^{\min(N,N-h)} e^{2\pi i h (g(n,h))\alpha} \right|^{8^{k-2}} e^{-2\pi i m |h| \alpha} d\alpha. \end{aligned}$$

We now set $\beta = \alpha |h|$ and hence $d\beta = d\alpha |h|$. We receive

$$\int_0^1 \left| \sum_{n=\max(0,-h)}^{\min(N,N-h)} e^{2\pi i (\operatorname{sgn} h)(g(n,h))\beta} \right|^{8^{k-2}} e^{-2\pi i m \beta} d\beta = \int_0^1 \left| \sum_{n=\max(0,-h)}^{\min(N,N-h)} e^{2\pi i (g(n,h))\beta} \right|^{8^{k-2}} e^{-2\pi i m \beta} d\beta.$$

This, combined with the induction hypothesis, gives

$$|C_m(h)| \leq \int_0^1 \left| \sum_{n=\max(0,-h)}^{\min(N,N-h)} e^{2\pi i (g(n,h))\beta} \right|^{8^{k-2}} d\beta \ll N^{8^{k-2}-(k-1)}.$$

By Lemma 5.5 we have

$$\begin{aligned} \int_0^1 \left(\sum_{\substack{h=-N \\ h \neq 0}}^{N} |b_h|^{8^{k-2}} \right)^4 d\alpha &= \int_0^1 \left(\sum_{\substack{h=-N \\ h \neq 0}}^{N} \sum_{|m| \leq CN^{k-1}} C_m(h) e^{2\pi i m h \alpha} \right)^4 d\alpha \\ &= \sum_{\substack{h_1,\ldots,h_4=-N \\ h_1,\ldots,h_4 \neq 0}}^{N} \sum_{|m_1|,\ldots,|m_4| \leq CN^{k-1}} \left(\prod_{i=1}^{4} C_{m_i}(h_i) \right) \int_0^1 e^{2\pi i \sum_{i=1}^4 m_i h_i \alpha} d\alpha \\ &= \sum_{\substack{h_1,\ldots,h_4=-N \\ h_1,\ldots,h_4 \neq 0 \\ h_1 m_1 + \cdots + h_4 m_4 = 0}}^{N} \sum_{|m_1|,\ldots,|m_4| \leq CN^{k-1}} \prod_{i=1}^{4} C_{m_i}(h_i) \\ &\ll N^{4(8^{k-2}-(k-1))} \sum_{\substack{h_1,\ldots,h_4=-N \\ h_1,\ldots,h_4 \neq 0 \\ h_1 m_1 + \cdots + h_4 m_4 = 0}}^{N} \sum_{|m_1|,\ldots,|m_4| \leq CN^{k-1}} 1 \\ &\ll N^{4(8^{k-2}-(k-1))} N^{3k} \\ &= N^{4 \cdot 8^{k-2} - k + 4}. \end{aligned}$$

Plugging these results into (11) we see that

$$\int_0^1 \left| \sum_{n=0}^{N} e^{2\pi i f(n)\alpha} \right|^{8^{k-1}} d\alpha \ll N^{4\cdot 8^{k-2}} + N^{4\cdot 8^{k-2}-4} N^{4\cdot 8^{k-2}-k+4}$$
$$\ll N^{4\cdot 8^{k-2}} + N^{8^{k-1}-k}.$$

Again, what we are after is to show that

$$\int_0^1 \left| \sum_{n=0}^{N} e^{2\pi i f(n)\alpha} \right|^{8^{k-1}} d\alpha \ll N^{8^{k-1}-k}$$

for $k \geq 2$. We need not consider the case $k = 2$ since it has already been shown. When $k \geq 3$ it is easy to see that $N^{8^{k-1}-k}$ dominates over $N^{4\cdot 8^{k-2}}$. Hence the theorem is proved. ■

We may now go back to Theorem 4.1, for which a proof was sketched in section 4. Now that proof is complete. Recall the set A which consists of all the positive integers N for which there is at least one solution such that

$$x_1^k + x_2^k + \cdots + x_h^k = n$$

where $1 \leq n \leq N$ and h is an integer which only depends on k. What we have proved in Theorem 4.1 is that the Shnirelman density of A, denoted $\sigma(A)$, is positive. Going back to Theorem 3.8, we see that if $\sigma(A) > 0$ and $0 \in A$, then A is a basis of finite order. That is, there is a p such that every positive integer n may be represented thus

$$(x_{11}^k + \cdots + x_{1h}^k) + (x_{21}^k + \cdots + x_{2h}^k) + \cdots + (x_{p1}^k + \cdots + x_{ph}^k) = n.$$

This means, of course, that the set A', which consists of all kth-powers, is a basis of finite order as well. ph such kth-powers will represent any positive number. To prove this was exactly the objective of this thesis. Hence we are done.

References

[1] G. H. Hardy and J. E. Littlewood, *A new solution of Waring's problem*, Quart. J. Math, Vol. 48 (1920)

[2] David Hilbert, *Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem)*, Mathematische Annalen, Vol. 67, No 3 (1909)

[3] Hua Loo Keng, *Introduction to Number Theory*, Springer (1982)

[4] Tim Jameson, *Linnik's Proof of the Waring–Hilbert Theorem from Hua's Book (with a Correction)*, `http://www.maths.lancs.ac.uk/ jameson/warlin.pdf` (2016.04.29).

[5] Yuri Vladimirovich Linnik, *An elementary solution of the problem of Waring by Schnirelman's method*, Matematicheskii Sbornik, Vol. 54, No 12 (1943)

[6] Melvyn B. Nathanson, *Additive Number Theory*, Springer (1996)

[7] R. C. Vaughan and T. D. Wooley, *Waring's Problem: A Survey*, Number theory for the millennium, Vol. 3 (2002)

[8] Edward Waring, *Meditationes Algebraic*, second edition, Archdeacon, Cambridge, (1770)