On Warings problem

Tomiris Kurmanlina

July 15, 2023

Intorduction

Waring's Problem, formulated by Edward Waring in 1770, is a significant problem in number theory, aiming to find the minimum number of k-th powers needed to represent any positive integer. It connects various mathematical fields and provides insights into the structure of numbers. The problem is related to perfect powers and has practical applications in cryptography and coding theory. Progress has been made for specific values of k, and computational methods have aided in understanding the behavior of the minimum number of k-th powers. Overall, Waring's Problem remains a captivating and important area of research in number theory.

History of problem and context

Hilbert was the first to solve Waring's Problem, followed by Hardy and Littlewood who proved that for any value of k, there exists an s such that every sufficiently large whole number can be expressed as a sum of s k-th powers. They also provided an approximate formula for the number of ways in which each whole number can be represented as such a sum. This formula improves its accuracy as the numbers being considered grow larger. In the context of the 18th century, Edward Waring formulated Waring's Problem during a time of significant mathematical development. Number theory, prime numbers, factorization, and perfect powers were popular topics of study. Waring was influenced by mathematicians like Lagrange and Euler, who made notable contributions to number theory and the representation of integers as sums of powers. Additionally, Fermat's Last Theorem and related problems drove further investigation into the properties of numbers and their representations.

Warings problem for squares

Theorem

Prove that for any positive integer k, there exists $g(k)$ such that every positive integer can be expressed as the sum of $g(k)$ perfect squares.

Proof

Proof.

To prove Waring's problem for squares, we can follow an inductive argument. Let's assume that for all positive integers n less than or equal to k, there exists a positive integer $g(k)$ such that every positive integer up to n can be written as the sum of $g(k)$ perfect squares.

Now, we need to show that for $n = k + 1$, there exists a positive integer $g(k + 1)$ such that every positive integer up to n can be expressed as the sum of $g(k + 1)$ perfect squares.

Consider the base case, where $n = 1$. We can write 1 as 1^2, which is a perfect square. Thus, the base case holds.

Now, let's assume that every positive integer up to $n = k$ can be expressed as the sum of $g(k)$ perfect squares. We need to prove that every positive integer up to $n = k + 1$ can also be written in this way. □

Proof

Proof.

Since $n = k + 1$, we have two cases:
Case 1: n is a perfect square ($n = m^2$, where m is a positive integer). In this case, we can simply write n as the sum of one perfect square: $n = m^2$. Thus, $g(k + 1) = 1$.
Case 2: n is not a perfect square. In this case, we can express n as the sum of two numbers: $n = a^2 + b$, where a is a positive integer and b is a positive integer less than or equal to $n - a^2$.
Since $b \leq n - a^2 = k - a^2 + 1$, the number b can be expressed as the sum of $g(k)$ perfect squares, by our assumption. Additionally, a^2 is a perfect square, so we can write it as the sum of one perfect square.
Hence, $n = a^2 + b$ can be expressed as the sum of $g(k) + 1$ perfect squares. □

Proof

Proof.

Therefore, by induction, we have shown that for any positive integer k, there exists a positive integer $g(k)$ such that every positive integer can be written as the sum of $g(k)$ perfect squares. This completes the proof of Waring's problem for squares. □

Warings problem for squares

Theorem

Prove that $g(k) = 4$ for Warings Problem for squares.

Lemma 1

Proof.

Firstly we will prove three lemmas.

Lemma

For any integers a, b, c, d, w, x, y, z,

$$(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2) =$$
$$(aw+bx+cy+dz)^2+(ax-bw-cz+dy)^2+$$
$$+(ay+bz-cw-dz)^2+(az-by+cx-dw)^2$$

□

This is the Euler four-square identity, with different notation.

Lemma 2

Lemma

If $2m$ is a sum of two squares, then so is m.

Proof.

Say $2m = x^2 + y^2$. Then x and y are both even or both odd. Therefore, in the identity
$m = ((x - y)/2)^2 + ((x + y)/2)^2$,
both fractions on the right side are integers. □

Lemma 3

Lemma

If p is an odd prime, then $a^2 + b^2 + 1 = kp$ for some integers a, b, k with $0 < k < p$.

Proof of Lemma 3

Proof.

Let $p = 2n + a$. Consider the sets
$A = a^2 | a = 0, 1, \ldots, n$ and $B = -b^2 - 1 | b = 0, 1, \ldots, n$.
We have the following facts:

1. No two elements in A are congruent $mod p$, for ir $a^2 \equiv c^2 (mod p)$, then either $p|(a - c)$ or $p|(a + c)$ by unique factorization of primes. Since $a - c, a + c \leq 2n < p$, and $0 \leq a, c$, we mush have $a = c$.
2. Similarly, no two elements in B are congruent $mod p$.
3. Furthermore, $A \cap B = \emptyset$ since elements of A are all non-negative, while elements of B are all negative.
4. Therefore, $C := A \cap B$ has $2n + 2$, or $p + a$ elements.

proof of lemma 3

Proof.

Therefore, by the pigeonhole principle, two elements in C must be congruent $mod p$. In addition, by the first two facts, the two elements must come from different sets. As a result, we have the following equation:

$$a^2 + b^2 + a = kp$$

for some k. Clearly k is positive. Also,
$p^2 = (2n+1)^2 > 2n^2 + 1 \geq a^2 + b^2 + 1 = kp$, so $p > k$.
Basically, Lemma 3 says that for any prime p, some multiple $0 < m < p$ of p is a sum of four squares, since $a^2 + b^2 + 1 = a^2 + b2 + a^1 + 0^2$. □

proof of theorem

Proof.

Proof of Theorem. By Lemma 1 we need only show that an arbitrary prime p is a sum of four squares. Since that is trivial for $p = 2$, suppose p is odd. By Lemma 3, we know

$$mp = a^2 + b^2 + c^2 + d^2$$

for some m, a, b, c, d with $0 < m < p$. If $m = 1$, then we are done. To complete the proof, we will show that if $m > 1$ then np is a sum of four squares for some n with $1 \leq n < m$.
If m is even, then none, two or all four of a, b, c, d are even; in any of those cases, we may break up a,b,c,d into two groups, each group containing elements of the same parity. Then Lemma 2 allows us to take $n = m/2$. □

proof of theorem

Proof.

Now assume m is odd but > 1. Write

$$w \equiv a(modm)$$

$$x \equiv b(modm)$$

$$y \equiv c(modm)$$

$$z \equiv d(modm)$$

where w, x, y, z are all in the interval $(-m/2, m/2)$. We have

$$w^2 + x^2 + y^2 + z^2 < 4 \cdot m^2/4 = m^2$$

$$w^2 + x^2 + y^2 + z^2 < 4 \equiv 0(modm).$$

proof of theorem

Proof.

So $w^2 + x^2 + y^2 + z^2 = nm$ for some integer non-negative n. Since $w^2 + x^2 + y^2 + z^2 < m^2, n < m$. In addition, if $n = 0$, then $w = x = y = z = 0$, so that $a \equiv b \equiv c \equiv d \equiv 0(modm)$, which implies $mp = a^2 + b^2 + c^2 + d^2 = m^q$, or that $m|p$. But p is prime, forcing $m = p$, and contradicting $m < p$. So $0 < n < m$. Look at the product $(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2)$ and examine Lemma 1. On the left is nm^2p. One the right, we have a sum of four squares, Evidently three of them

$$ax - bw - cz + dy = (ax - bw) + (dy - cz)$$

$$ay + bz - cw - dx = (ay - cw) + (bz - dx)$$

$$az - by - cx + dw = (az - dw) + (cx - by)$$

proof of theorem

Proof.

are multiplies of m. The same is true of the other sum on the right in Lemma 1:

$$aw + bx + cy + dz \equiv w^2 + x^2 + y^2 + z^2 \equiv 0(modm).$$

The equiation in Lemma 1 can therefore be divided through by m^2. The result is an expression for np as a sum of four squares. Since $0 < n < m$, the proof is complete. □

Thank you for your attention!