What is ... Waring's Problem

Allison Paul
Sandeep Silwal

07/16/2015

Abstract

In 1770 Lagrange proved his famous theorem that every natural number can be written as the sum of 4 squares. In the same year, Edward Waring in his *Meditationes Algebraicae* cojectured a generalization that every natural number can be written as the sum of at most s kth powers. This came to be known as Waring's Problem. In this talk, we overview the early solutions given by Hilbert and then Hardy and Littlewood as well as present an elementary solution given by Y. V. Linnik. We also explore some interesting generalizations such as the "Waring-Goldbach problem".

1 History

In 1640, Fermat conjectured that every positive integer can be written as the sum of four squares. Euler attempted to to solve this problem but was unsucessful. However, he was was able to reduce this problem to primes by using his four square identity that he discovered in 1748. Finally in 1770, Lagrange showed that every positive integer can be expressed as the sum of 4 squares, and in the same year, Edward Waring in his book *Meditationes Algebraicae* made the remarkable conjecture that "Every number is the sum of 4 squares; every number is the sum of 9 cubes; every number is the sum of 19 fourth powers; and so on[3]." Furthermore, in his 1782 edition, Waring somewhat mysteriously added that "similar laws may be affirmed for the correspondingly defined numbers of quantities of any like degree[3]." This conjecture came to be known as Waring's problem.

Waring's Problem. *For all $k \in \mathbb{N}$, there exists a $g(k)$ such that every $a \in \mathbb{N}$ can be expresseed as the sum of at most $g(k)$ kth powers of positive integers.*

2 Early Works and Hilbert's Proof

Due to Waring's mysterious quote, there is speculation that Waring was referring to polynomial expressions and was not limiting his conjectures to only nth powers.. A result of this nature was proven by Erich Kamke in 1921.[5]

Theorem (Kamke, 1921). *Let $f(x)$ be an integer valued polynomial with no fixed divisor $d > 1$ (i.e., there is no such d such that $d|f(n)\ \forall n \in \mathbb{N}$). Then for large enough s,*

$$f(x_1) + f(x_2) + \cdots + f(x_s) = n$$

is solvable for large enough n.

We now return our focus back to Waring's problem. During the next 139 years after Waring's claim, only special cases of his conjecture were proved for $k = 3, 4, 5, 6, 7, 8, 10$ and using Lagrange's work, Joseph Liouville in 1859 was able to show that $g(4) \leq 53$. It was only in 1909 that Hilbert was able to show that $g(k)$ exists for all k. Hilbert's proof used geometrical results about convex bodies to show that every sufficiently large positive integer can be written as a rational combination of a fixed number of *kth* powers. Hilbert then showed that this was equivalent to Waring's problem. However, Hilbert's proof provided no insights on the bounds for $g(k)$ and only in 1953 did G. Rieger prove the unwieldy bound (given in [3])

$$g(k) \leq (2k+1)^{260(k+3)^{3k+8}}.$$

3 Hardy and Littlewood

A decade after Hilbert's proof, Hardy and Littlewood used a very different technique called the circle method to solve Waring's problem. This method arose from Hardy and Ramanujan and their study of the partition function in 1918 which appeared the

paper *Asymptotic Formulae in Combinatory Analysis*. This method was utilized by Hardy and Littlewood in their solution of Waring's problem in 1920. We will present a quick sketch of their proof.
Let

$$F(z) = \sum_{a=0}^{\infty} z^{a^k}$$

where $|z| < 1$. Then

$$F(z)^n = \sum_{a_1=0}^{\infty} \cdots \sum_{a_n=0}^{\infty} z^{a_1^k + \cdots a_n^k} = \sum_{m=0}^{\infty} r_n(m) z^m$$

where $r_n(m)$ is the number of nonnegative solutions to

$$m = a_1^k + a_2^k + \ldots + a_n^k. \tag{1}$$

Then using Cauchy's integral formula, we have

$$r_n(m) = \frac{1}{2\pi i} \int_C F(z)^n z^{-m-1} dz$$

where C is a circle centered at the origin with radius $0 < \rho < 1$. The problem in evaluating this integral arises from the singularities $e^{\frac{2\pi i p}{q}}$ for all rationals $\frac{p}{q}$. The "heaviest" singularities are at the points where q has a small denominator. To get around this problem, Hardy and Littlewood divided the circle into major and minor arcs which allowed them to estimate this integral. They were able to show that $r_n(m)$ has order of magnitute $m^{\frac{n}{k}-1}$ so for all m, $r_n(m) > 0$ for sufficiently large $n = g(k)$. In an essay, Hardy himself described the circle method as

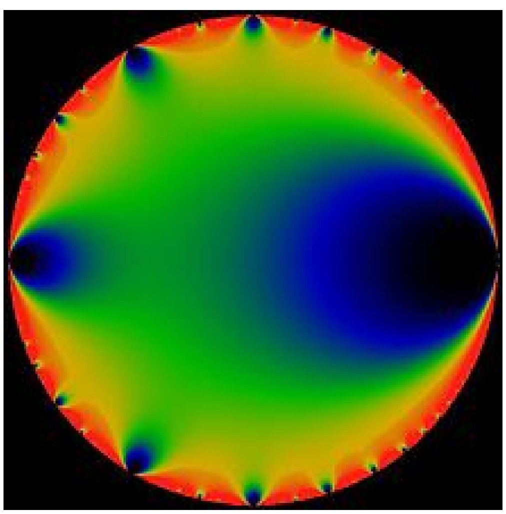

Figure 1: Singularities in the Unit Circle (Courtesy of Wikimedia)

"Imagine the unit circle as a thin circular rail, to which are attached an infinite number of small lights of varying intensity, each illuminating a certain angle immediately in front of it. The brightest light is at $x = 1$, corresponding to $p = 0, q = 1$; the next brightest at $x = -1$, corresponding to $p = 1, q = 2$; the next at $x = e^{\frac{2\pi i}{3}}$ and $e^{\frac{4\pi i}{3}}$, and so on. We have to arrange the inner circle, the circle of integration, in the position of maximum illumination. If it is too far away the light will not reach it; if too near, the arcs which fall within the angles of illumination will be too narrow, and the light will not cover it completely. Is it possible to place it where it will receive a satisfactorily uniform illumination?[1]"

4 Approximations and Variations

Hardy and Littlewood's method of approximating $r_n(k)$ allowed others to establish bounds for $g(k)$. For example, Balasubramanian proved that $g(4) = 19$ (1986) and

Chen proved that $g(5) = 37$ (1964)[9]. Dickson, Pillai, and Niven also conjectured that for $k > 6$,

$$g(k) = 2^k \left\lfloor (3/2)^k \right\rfloor - 2$$

when

$$2^k\{(3/2)^k\} + \left\lfloor (3/2)^k \right\rfloor \leq 2^k.$$

Interestingly, this value for $g(k)$ was proposed as a lower bound by J.A. Euler, son of Leonhard Euler. Mahler in 1957 showed that the above conjecture holds for all n except a finitely many exception and as of 1989, this has been verified for $k \leq 471,600,000$[9]!

Now instead of asking for the value of $g(k)$, we can ask a slightly modified question: How many kth powers does it take to write every sufficiently large integer as the sum of kth powers? Denote this value as $G(k)$. It is known that $G(2) = 4, G(4) = 16$ and $G(3) \leq 7$[1]. Hardy and Littlewood were able to prove that

$$G(k) \leq (k-2)2^{k-1} + 5.$$

The most recent upper bound for $G(k)$ was given by Trevor Wooley in 1992 and he was able to show[8]

$$G(k) \leq k \log k + k \log \log k + Ck$$

for some constant C. We can extend our question to ask for the value of $G_1(k)$ which is the number of kth powers such that *almost all* numbers can be expressed as a sum of $G_1(k)$ kth powers. (Here *almost all* means an asymptotic density of 1). It is known that $G_1(2) = 4, G_1(3) = 4, G_1(4) = 15$ but further research is needed.
Even though Hardy and Littlewood's methods gave reasonable bounds for $g(k)$, we would still like an elementary solution since the statement of Waring's problem is so simple. Such an elementary proof was given by the Soviet scholar Y. V. Linnik in 1940 using the ideas of Lev Schnirelmann developed in 1936.

5 Schnirelmann's Inequality

Before presenting Linnik's elementary proof, we must first discuss the idea of a basis and the density of a set. Recall that Lagrange's Four Square theorem states that every positive integer can be written as the sum of at most four squares. Another interpretation of this statement is that $\mathbb{N} = A + A + A + A$ where A is the set of all nonegative squares. In general, we will say that a set S is a basis of $\mathbb{N}$ if

$$\mathbb{N} = \underbrace{S + \ldots + S}_{j}$$

for some natural number j. Waring's problem then can be reformulated as the kth powers form a basis in the natural numbers. Now for a set S, define

$$S(n) = \#\{s_i \in S : 1 \leq s_i \leq n\}.$$

Schnirelmann then defined the density of S as

$$d(S) = \inf_n \frac{S(n)}{n}.$$

He then proved the following inequality.

Theorem (Schnirelmann, 1936). *Let $A, B \subseteq \mathbb{N}$. Then*

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

Using the pigeonhole principle, Schnirelmann then proved the following theorem.

Theorem (Schnirelmann, 1936). *If $A, B \subset \mathbb{N}$ and $0 \in A \cap B$ then*

$$A(n) + B(n) > n - 1$$

implies $n \in A + B$.

Using the two previous results, Schnirelmann was able to arrive at the following theorem.

Theorem (Schnirelmann, 1936). *Every sequence of positive density is a basis of* $\mathbb{N}$.

Now let $A_k = \{a^k : a \in \mathbb{N}\}$. If we prove that the density of

$$A_k^n = \underbrace{A_k + \cdots + A_k}_{n}$$

is positive for some j, then Waring's problem follows. In an interesting note, Henry Mann in 1942 was able to prove the stronger statement:

Theorem (Mann, 1942). *Let $A, B \subseteq \mathbb{N}$. Then*

$$d(A+B) \geq d(A) + d(B)$$

provided that $d(A) + d(B) \leq 1$. If $d(A) + d(B) \geq 1$, then we have $d(A+B) = 1$.

6 Linnik's Elementary Proof

Linnik's proof is based on the fact that A_k^n has positive density for sufficiently large n. If we show that, then we are done since we know from Schnirelmann's thoerem above that this means A_k forms a basis of $\mathbb{N}$. Now recall that $r_k(m)$ denotes the number of solutions(1). Most of the work in Linnik's proof is hidden in the following claim.

Fundamental Lemma. *There exists a natural number k depending only on n, and a constant c, such that for all $N \geq 1$,*

$$r_n(m) < cN^{(n/k)-1} \qquad (1 \leq m \leq N).$$

The proof of the Fundamental Lemma is very tedious so we will take it as a black box. ([6] gives a proof of this lemma.) Linnik then showed that the Fundamental Lemma implied that $d(A_k^n) > 0$ for some large n. To do this, he defined

$$\begin{aligned} R_n(N) &= r_n(0) + r_n(1) + \cdots + r_n(N) \\ &= \#\{a_1^k + a_2^k + \cdots + a_n^k \leq N\}. \end{aligned}$$

By counting the number of possibilities to each a_i, Linnik was able to show that

$$R_n(N) \geq \left(\frac{N}{n}\right)^{n/k}$$

so $R_n(N)$ is relatively large as N is arbitrary. Linnik's arguments then can be summeraized as follows. If $d(A_k^n) = 0$, then the number of integers m for which $r_n(m) > 0$ is small. The Fundamental Lemma gives us that $r_n(m) < cN^{(n/k)-1}$ so $R_n(N)$ would be relatively small. However, $R_n(N)$ is arbitarily large, which would give us a contradiction. Thus, $d(A_k^n)$ must be positive and Waring's problem is proved. This lemma is interesting in other contexts besides Waring's problem since it also holds for an arbitary sum of polynomial equations. That is, if

$$f(x_1) + f(x_2) + \cdots + f(x_n) = m$$

then the number of solutions, $r_n(m)$ also satisfies the Fundamental Lemma.[5]

7 Generalizations

Waring's problem has been generalized in different directions. In 1938, using methods similar to that of Vinogradov, Hua Luogeng proved the following.[3]

Theorem (Hua, 1938). *For $k \in \mathbb{Z}^+$ and for large enough N, we have*

$$N = p_1^k + p_2^k + \cdots + p_t^k$$

where p_i's are primes and $t \leq g(k)$.

This is often called the "Waring-Goldbach" problem. One known result relating to Hua's work is that every sufficiently large odd integer is the sum of 21 fifth powers of primes[3].

Another interesting direction to generalize Waring's problem was by E. Scourfield in 1960.[3]

Theorem (Scourfield, 1960). *If $n_1 \leq n_2 \leq \cdots$ is a sequence of positive integers, then there exists a $k \in \mathbb{Z}^+$ such that every positive integer N can be written as*

$$N = \sum_{i=1}^{r} x_i^{n_{i+k}} \quad x_i \in \mathbb{Z}^+$$

for some fixed constant r if and only if $\sum_{i=1}^{\infty} \frac{1}{n_i}$ diverges.

There is also a variant of Waring's problem in real fields and algebraic number fields given in [7] as well as one where the kth powers come only from Beatty sequences which can be found in [2].

8 References

[1] Hardy, G. H. "Some Famous Problems of the Theory of Numbers and in Particular Waring's Problem: An Inaugural Lecture Delivered before the University of Oxford." Nature 106.2660 (1920). Web.
[2] Banks, William D., Ahmet M. Güloğlu, and Robert C. Vaughan. "Waring's Problem for Beatty Sequences and a Local to Global Principle." J. Théor. Nombres Bordeaux Journal De Théorie Des Nombres De Bordeaux 26.1 (2014): 1-16. Web.

[3] Ellison, W. J. “Waring’s Problem.” The American Mathematical Monthly 78.1 (1971): 10. Web.
[4] Ellison, William. “Waring’s Problem for Fields.” Acta Arithmetica. 159.4 (2013): 315-30. Web.
[5] Ford, K. “Waring’s Problem with Polynomial Summands.” Journal of the London Mathematical Society 61.3 (2000): 671-80. Web.
[6] Khinchin, A. Three Pearls of Number Theory. Rochester, NY: Graylock, 1952. Print.
[7] Siegel, Carl Ludwig. “Generalization of Waring’s Problem to Algebraic Number Fields.” American Journal of Mathematics 66.1 (1944): 122. Web.
[8] Vaughan, R. C.; Wooley, T. D. Waring’s problem: a survey. Number theory for the millennium, III (Urbana, IL, 2000), 301–340, A K Peters, Natick, MA, 2002.
[9] “Waring’s Problem.” – from Wolfram MathWorld. Web.
`http://mathworld.wolfram.com/WaringsProblem.html.`