WARING'S PROBLEM AND RESULTS

[redacted]

ABSTRACT. Waring's problem although simple took over a century to prove in general. The problem's history and definition is presented along with a two proofs. First, that any integer is a sum of at most four squares. Second, an elementary proof which proves Waring's problem for all cases.

1. INTRODUCTION

Edward Waring is best known for a problem concerning sums of positive integers raised to positive k powers. He was a Lucasian chair of mathematics at Cambridge, a Fellow of the Royal Society, and received the Royal Society Copley Medal for achievements in mathematics. Surprisingly he presented his conjecture, aptly called Waring's problem, without proof.

In 1770, Waring stated that any positive integer can be written as the sum of no more than a fixed m of positive kth integer powers [1]. He states that every positive integer is the sum of four squares, nine cubes, nineteen powers of four and so on. For convenience we denote m by

$$g(k) = m$$

Later that same year Lagrange proved that Waring's conjecture when k=2 was true, that is every positive integer is the sum of at most four squares.

Two years later Euler gives a lower bound for $g(k)$ calculated by

$$\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + 2^k - 2 \tag{1}$$

Throughout the 19th century work from J. Liouville [3], E. Lucas [4], and many others contributed to determining m for k=3, 4, 5, and 6. It was not until 1909 when a proof regarding the existence of such an m for any positive integer k was presented by D. Hilbert [5]. His proof relied on complicated analysis and multiple integrals.

A few years later G.H. Hardy and J.E. Littlewood [6]

> "... made use of the theory of analytic functions to prove that every positive integer, which exceeds a certain number depending on k alone, is a sum of at most $k^{2k-1}+1$ positve *kth* powers; for example, a sum of at most 33 biquadrates. The transcendental method leads not only to a proof of the existence of representations, but also to asymptotic formulas for their number." [10]

Using this method, it has has been shown that (1) is in fact $g(k)$ for $6 \leqslant k \leqslant 471600000$ [7]. Thus Euler's equation is generally believed to be the exact value of $g(k)$.

2. PROOF THAT EVERY POSITIVE INTEGER IS THE SUM OF AT MOST FOUR SQUARES

When k=1, $g(k) = 1$ since for $n \in \mathbb{N}$ we have

$$n^1 = n.$$

Therefore we are concerned with the more interesting cases where $k \geqslant 2$.

The simplest such case is when $k = 2$. Lagrange proved that every positive integer is the sum of at most four squares i.e. $g(2) = 4$ in the same year Waring publicized his conjecture.

To see that this is true, first note that

$$1 = 1^2 + 0^2 + 0^2 + 0^2.$$

Let $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ and $y_1, y_2, y_3, y_4 \in \mathbb{Z}$. Then the product

$$(2) \qquad (x_1 + x_2 + x_3 + x_4)(y_1 + y_2 + y_3 + y_4) = a^2 + b^2 + c^2 + d^2$$

is itself a product of four squares where $a = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$, $b = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3$, $c = x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4$, and $d = x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2$.

So it is equivalent to show that for any prime p, p is the sum of at most four squares.

When $p = 2$, $2 = 1^2 + 1^2 + 0^2 + 0^2$. Thus assume $p > 2$.

We will also require the following (proof left to reader)

Theorem 2.1. *If p is an odd prime, then there are numbers x and y such that*

$$1 + x^2 + y^2 = mp \quad (0 < m < p).$$

Thus there is some $m \in \mathbb{Z}$ such that

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

where x_1, x_2, x_3, x_4 are all relatively prime to p.
We now wish to show that p is the least such multiple.

Let m_0p be the least such multiple. If $m_0 = 1$ our proof is complete. Assume $m_0 > 1$. From above, $0 < m_0 < p$.
Suppose m_0 is even.

Then the sum of $x_i's$ is even. Thus the $x_i's$ are:
(i) all even
(ii) all odd
(iii) two are even and two are odd

Suppose without loss of generality that for (iii), x_1, x_2 are even and x_3, x_4 are odd. Then

$$x_1 + x_2, x_1 - x_2, x_3 + x_4, x_3 - x_4$$

are all even for each case i, ii, and iii.

So

$$\frac{1}{2}m_0p = (\frac{x_1 + x_2}{2})^2 + (\frac{x_1 - x_2}{2})^2 + (\frac{x_3 + x_4}{2})^2 + (\frac{x_3 - x_4}{2})^2$$

is the sum of four integer squares. No square is divisible by p since each x_i is not divisible by p. This contradicts our definition of m_0.

Thus m_0 must be odd.

Each of x_1, x_2, x_3, x_4 are not divisible by m_0.
Otherwise $m_0^2 \mid m_0p$ and that implies $m_0 \mid p$.
Furthermore m_0 is odd and $m_0 > 1$, $m_0 \geqslant 3$.

Now we wish to choose some b_1, b_2, b_3, b_4 such that

$$y_i = x_i - b_i m_0 \quad (i = 1, 2, 3, 4)$$

satisfies the inequalities

$$|y_i| < \frac{1}{2}m_0, \quad y_1^2 + y_2^2 + y_3^2 + y_4^2 > 0.$$

Then

$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4(\frac{1}{2}m_0)^2,$$

and

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m_0}.$$

So

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= m_0 p \quad (m_0 < p), \\ y_1^2 + y_2^2 + y_3^2 + y_4^2 &= m_0 m_1 \quad (0 < m_1 < m_0). \end{aligned}$$

From equation (2) let

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

Then

$$m_0^2 m_1 p = z_1^2 + z_2^2 + z_3^2 + z_4^2 \tag{3}$$

But

$$z_1 = \sum x_i y_i = \sum x_i(x_i - b_i m_0) \equiv \sum x_i^2 \equiv 0 \bmod m_0$$

Similarly, z_2, z_3, z_4 are divisible by m_0. So we may write

$$z_i = m_0 j_i \quad (i = 1, 2, 3, 4).$$

Thus (3) becomes

$$m_1 p = j_1^2 + j_2^2 + j_3^2 + j_4^2.$$

But this contradicts the definition of m_0 because $m_1 < m_0$.
Therefore $m_0 = 1$ and we conclude that p is the sum of at most four integers squared.

3. An general proof for Waring's problem

The purpose of the proof given here is to prove the existence of m such that $g(k) = m$ for any $k \in \mathbb{N}$. It comes from a 20th century mathematician named Y.V. Linnik. This elementary proof relies on L. G. Schnirelmann's theorem

Theorem 3.1. *Every sequence of positive density is a basis of the sequence of natural numbers.*

Recall that a sequence S is *a basis of order* k if the sum of k identical sequences S contains all the natural numbers.

The concept of density is not as simple.

Let S be the sequence $0, s_1, s_2, \ldots, s_n, \ldots$ where $i = 1, 2, 3, \ldots$, $s_i \in \mathbb{N}$ and $s_i < s_{i+1}$. Let $S(n)$ indicate the number of natural numbers in S that do not exceed n so that $0 \leqslant S(n) \leqslant n$.

Then upon multiplication by $\frac{1}{n}$ we have the inequality

$$0 \leqslant \frac{S(n)}{n} \leqslant 1,$$

which is different for each n. [8]

For example let $S' = 0, 2, 3, 5, 7, 11, \ldots$ i.e. S' is a sequence of the prime numbers. Then $S'(13) = 5$ and

$$0 \leqslant \frac{5}{13} \leqslant 1.$$

Consider $\frac{S'(n)}{n}$ for all n. The greatest lower bound of that set of numbers is the density of the sequence S'.

More formally,

Definition 3.2. The density of the sequence S, denoted by $d(S)$, is the greatest lower bound of all values of $\frac{S(n)}{n}$.

The Schnirelmann theorem states that if $d(S) > 0$ then the sum of a sufficiently large number of sequences S contains the entire sequence of natural numbers. Thus to show (1) for any $k \in \mathbb{N}$ we may show that the sequence $s_1^k, s_2^k, \ldots, s_m^k$ has density greater than 0.

Before stating the proof we state the following lemma

Lemma 3.3. *There exists a natural number $k = k(n)$, depending only on n, and a constant c, such that, for an arbitrary $N \in \mathbb{N}$,*

$$(4) \qquad r_m < N^{\frac{k}{n}} - 1 \qquad (1 \leqslant m \leqslant N).$$

Now, by definition of $r_k(m)$ from the lemma, the sum

$$(5) \qquad r_k(0) + r_k(1) + \cdots + r_k(N) = R_k(N)$$

gives the number of systems $(x_1^n + x_2^n + \ldots + x_k^n \geqslant N$. Every group of numbers for which $0 \geqslant x_i \geqslant (\frac{N}{k})^{1/n}(1 \geqslant i \geqslant k)$, obviously satisfies this condition. To satisfy these inequalities, every x_i can evidently be chosen in more than $(N/k)^{1/n}$ different ways $(x_i = 0, 1, \ldots, \lfloor (N/k)^{1/n} \rfloor)$. After an arbitrary choice of this sort, the numbers $x_1, x_2, \ldots, x_k$ may be combined, and so we have more than $(N/k)^{k/n}$ different possibilities for choosing the complete system of integers x_i $(1 \geqslant i \geqslant k)$ so as to satisfy condition (3). This shows that

$$(6) \qquad R_k(N) \geqslant (N/k)^{k/n}.$$

We assume that the fundamental lemma has been shown to be correct, and that inequality (2) is satisfied for an arbitrary N. We now have to verify that inequality (2) is consistent with inequality (4) which we proved, only if the sequence $A^{(}_{n}k)$ has a positive density.

So now assume that $d(A_n)^k = 0$. For an arbitrarily small $\alpha > 0$ and a suitably chosen N,

$$A_n^k(N) < \alpha * N.$$

From the following theorem we may assume that N is arbitrarily large since $1 \in A_n^k$.

Theorem 3.4. *If $d(S) = 0$ and S contains the number 1, and if $\alpha < 0$ is arbitrary, then there exists a sufficiently large t such that $S(t) < \alpha * t$.*

We apply the inequality (2) to get

$$\begin{aligned} R_n(N) &= \sum r_k(m) \\ &= r_k(0) + \sum r_k(m) \\ &< 1 + cN^{k/n} - 1A_n^k(N) \\ &< 1 + c\alpha * N^{k/n}. \end{aligned}$$

Thus for sufficiently large N,

$$R_k(N) < 2c\alpha * N^{k/n}.$$

For sufficiently small α,

$$2c\alpha < \frac{(\frac{1}{k})^k}{n},$$

so that

$$R_k(N) < (\frac{N}{k})^{k/n}.$$

This contradicts (4) hence $d(A_n^k) > 0$. [9]
Therefore by the Schnirelmann theorem we have shown that $g(k) = m$ for $m \in \mathbb{N}$ and $k \in \mathbb{N}$.

This paper discussed a small fraction of a very deep problem. For example, recall that Euler suggested that $\lfloor(\frac{3}{2})^k\rfloor + 2^k - 2$ is a lower bound for $g(k)$. To date Waring's problem epitomizes the nature of many problems of number theory. That is, they are simple to describe, accessible to puzzlers and mathematicians, but have vast implications that often take many years to fully describe.

References

[1] Meditationes algebraicae, Cambridge, 1770, 204-5; ed.3, 1782, 349-250

[2] Opera postuma, 1, 1862, 203-4 (about 1772)

[3] In his lectures at the Collège de France; printed in V.A. Lebesque's Exercices d'Analyse Numérique, Paris, 1859, 112-5. Cf. E. Maillet, Bull. Soc. Math. France, 23, 1895, bottom of p. 45

[4] Nouv. Corresp. Math., 2, 1876 ,101

[5] Göttingen Nachr., 1909, 17-36; Math. Ann., 67, 1909, 281-300

[6] Quar. Jour. Math., 48, 1919, 272 seq.

[7] Kubina, J. M. and Wunderlich, M. C. "Extending Waring's Conjecture to 471600000." Math. Comput. 55, 815-820, 1990.

[8] A. Y. Khinchin, *Three Pearls of Number Theory*, 1st edition, Graylock Press, New York 1952, p. 21-22

[9] A. Y. Khinchin, *Three Pearls of Number Theory*, 1st edition, Graylock Press, New York 1952, p. 40-41

[10] L.E. Dickson, *History of the Theory of Numbers, Volume II: Diophantine Analysis*, 2nd edition, G.E. Stechert and Co., New York 1934

[11] M. Gardner, *Knotted Doughnuts and Other Mathematical Entertainments*, 1st edition, W.H. Freeman and Co., New York 1986.

[12] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, 5th edition, Oxford University Press, Oxford 1979.

The Ohio State University
E-mail address: [redacted]