Waring's problem, taxicab numbers, and other sums of powers

8 Dec 2004

1. Introduction. Many of the most perplexing problems in number theory arise from the interplay of addition and multiplication. One important class of such problems is those in which we ask which numbers can be expressed as *sums* of some numbers which are defined *multiplicatively*. Such classes of numbers include nth powers (in this paper, for any fixed n; in a more general treatment, n could also be variable). This gives rise to the Pythagorean theorem known by every schoolchild as well as the much more perplexing problem of Fermat, the so-called "Hardy-Ramanujan" or "taxicab" numbers, the four-square theorem of Lagrange, Waring's problem, and various other famous number-theoretic problems. If we attempts to express numbers as sums of *primes*, we get the (still unproven) conjecture of Goldbach.

In this paper, I will begin by considering the most ancient of such problems, that of expressing a square as a sum of two squares. I give some results on which numbers can be expressed as a sum of two squares in various numbers of ways, using some elementary results from the theory of quadratic forms. And I will show which numbers can be expressed as sums of three squares (most, due to Gauss) and four squares (all, due to Lagrange). I will then examine the problem that made the number 1729 famous – which numbers are sums of two cubes in two different ways? I will present a probabilistic approach to predicting the number of solutions to this problem. I will give bounds on the number of ways of writing a number as a sum of two cubes, both based on its size and on its factorization. And I will present parametrizations that gives infinite families of solutions.

Finally, I will address what is usually known as "Waring's problem" – how many nth powers are needed to write any number as a sum of such powers? We will see the basic results for small powers of positive integers, including the variation of this problem known as the "easier" Waring problem in which sums and differences of powers are taken.

2. Pythagoras and Fermat. The Pythagorean theorem was known to Euclid ([**4**, Prop I.47]), but he seems to have treated it as a purely geometric proposition. And various sources repot that the ancient Egyptians knew about the existence of the 3-4-5 right triangle. What they may now have known is that there are infinitely many such triples, or that there is a simple parametrization of the same.

Let a *Pythagorean triple* be an ordered triple of positive integers (x, y, z) such that $x^2 + y^2 = z^2$. Then the simple algebraic identity

$$(r^2 - s^2)^2 + (2rs)^2 = (r^2 + s^2)^2 \tag{2-1}$$

gives an infinity of Pythagorean triples $(r^2 - s^2, 2rs, r^2 + s^2)$ where r and s are positive integers. What is perhaps more surprising is that all Pythagorean triples can be expressed in this form – and therefore the problem of generating a list of these is trivial. The following discussion is adapted from [**7**].

We note that the equation in question is homogeneous of degree 2, so if (x, y, z) is a Pythagorean triple, so is (kx, ky, kz) for any positive integer k. We define a *primitive Pythagorean triple* or PPT to be one such that $gcd(x, y, z) = 1$, and consider the problem of finding all primitive triples. The solution is as follows:

Theorem 1. *(x, y, z) is a PPT with y even if and only if $(x, y, z) = (r^2 - s^2, 2rs, r^2 + s^2)$ for some positve relatively prime integers r, s of opposite parity.*

Proof: We note that in a primitive triple, x, y cannot both be even, for then z would be even and the triple would not be primitive. But they cannot both be odd, for then $x^2 \equiv y^2 \equiv 1 \pmod 4$, and so $z^2 \equiv 2 \pmod 4$, which is impossible. So x and y are of opposite parity; since the equation is symmetric in x, y we will assume y is even and x is odd (and hence z is odd). Now, we will rewrite the equation as $(z - x)(z + x) = y^2$, and we note that all the exponents in the prime factorization of y^2 are even. We note that $z - x, z + x$ are both even, and rewrite to get

$$\frac{z + x}{2}\frac{z - x}{2} = \left(\frac{y}{2}\right)^2 \tag{2-2}$$

and since $(x, z) = 1$, the two factors on the left are relatively prime. And it is well-known that two relatively prime integers whose product is a square must be squares. So we get $(z + x)/2 = r^2, (z - x)/2 = s^2, y/2 = rs$ for some positive integers r, s; furthermore, $(r, s) = 1$ and $r > s$. And $r^2 - s^2 = x$ is odd, so r, s are of opposite parity. □ □

This gives an example of a parametric solution to a Diophantine equation; we will see others. We also see which *squares* can be represented as sums of two squares; we wll later take up the question of which integers can be expressed in like manner.

3. Numbers which are sums of squares. The central result of this section is that every positive integer can be expressed as a sum of four squares of nonnegative integers in at least one way.

We begin with some probabilistic results. (For further detail see [**6**].) Let $R_k(n)$ denote the number of k-tuples $(x_1, \cdots, x_k)$ of nonnegative integers such that $\sum_i x_i^2 \le n$. Thus, for example, $R_2(10) = 13$, with the pairs

$$(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3), (2,0), (2,1), (2,2), (3,0), (3,1).$$

Then we claim that $R_2(n) \approx \pi n/4$. We observe that pairs (x_1, x_2) such that $0 \le x_1, x_2$ and $x_1^2 + x_2^2 \le n$ correspond to points in that part of the circle of radius $\sqrt{n}$ centered on the origin which are in the first quadrant, and the number of these is very near the area of that quarter-circle, which is $\pi n/4$. Similarly, we predict $R_3(n) \approx \pi n^{3/2}/6$ (one-eighth the volume of a sphere of radius $n^{1/2}$) and $R_4(n) \approx \pi^2 n^2/2$. (Incidentally, the two-dimensional version of this problem is often known as the "circle problem", and it is possible to get an error term, but this seems irrelevant here.) The increasing exponents on n in these functions is a heuristic indication that there exists an integer k such that all positive integers are sums of k squares.

This probabilistic method predicts that the average number of representations of an integer near n as a sum of two squares is $\pi/4$; of three squares $\pi\sqrt{n}/4$; of four squares

$\pi^2 n$. But this method does not take into account purely number-theoretic considerations such as modular arithmetic; nor does it take into account that most k-tuples are counted "more than once" in $R_k(n)$ due to the inherent symmetry of the problem. For sums of two squares, we actually have the following characterization:

Theorem 2. *([**7**, p.55], originally due to Fermat) A positive integer n can be written as the sum of two integer squares if and only if all primes congruent to 3 modulo 4 occur in its prime factorization with an even exponent.*

Proof: (Sketch.) We note that $2 = 1^2 + 1^2$. It is known that all primes congruent to 1 modulo 4 can be written as a sum of two squares; a proof can be found in any standard number theory text. And for primes q, $q \equiv 3 \pmod 4$, $q^2 = q^2 + 0^2$ is a sum of two squares. Furthermore, we have the identity

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 \tag{3-1}$$

so if m and n are sums of two squares, then mn is as well. This proves that our condition is sufficient. The proof of necessity is omitted. □

A natural question to ask is: what is the probability that a randomly chosen integer can be written as a sum of two squares? The result, as found in [**5**, p.22], is due to Landau: let $N_2(x)$ be the *number* of integers less than x which are sums of two squares. (Note that $N_2(x)$ is not the same as $R_2(x)$, and in fact $N_2(x) < R_2(x)$ for all $x \geq 25$.) Then

$$N_2(x) = b\frac{x}{\sqrt{\log x}}\left[1 + \frac{c_1}{\log x} + \frac{c_2}{\log^2 x} + \cdots + \frac{c_n}{\log^n x} + O\left(\frac{1}{\log^{n+1} x}\right)\right]$$

for some real constants $b, c_1, c_2, \ldots$, and the constant b is

$$b = \left(\frac{1}{2}\prod_{q \equiv 3 \pmod 4}(1 - q^{-2})^{-1}\right)^{-1/2}$$

which has numerical value about $0.764223653\ldots$ and is known as the Landau-Ramanujan constant [**13**]. If we approximate $N_2(x)$ as $bx/\sqrt{\log x}$, then the probability of a number near x being a sum of two squares can be obtained by differentiation, giving

$$N_2'(x) \approx B\left(1 - \frac{1}{2\log x}\right)(\log x)^{-1/2}$$

so for large x the probability approaches zero, albeit rather slowly; $N_2'(10^{100}) \approx 0.05$, so one in every twenty numbers around 10^{100} is a sum of two squares.

The analogous classification of numbers that can be expressed as sums of *three* squares is due to Gauss:

Theorem 3. *([**7**, p. 170]; originally due to Gauss) An integer n can be written as the sum of three squares if and only if it is not of the form $4^m(8k + 7)$.*

Proof: First, we note that all squares are congruent to 0, 1, or 4 modulo 8. Thus, by adding the possible combinations of three of these, we see that no three of these give a sum of 7, so an integer congruent to 7 modulo 8 cannot be written as a sum of three squares. Incidentally, there is no identity like (3-1) or (3-2) for sums of three squares,

and in fact it is possible to find two numbers which can be written as a sum of three squares whose product cannot. For example, $3 = 1^2 + 1^2 + 1^2$, $21 = 4^2 + 2^2 + 1^2$, but $63 \equiv 7 \pmod 8$.

Now, if $x^2 + y^2 + z^2 = n$ and $4|n$, then considering $x^2, y^2, z^2 \pmod 4$, we see that $x^2, y^2, z^2 \equiv 0 \pmod 4$, so x, y, z are even. Thus, if n is a sum of three squares $n = x^2 + y^2 + z^2$, then

$$\frac{n}{4} = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2$$

gives $n/4$ as a sum of three squares. We can conclude that if $n = 4^m(8k + 7)$ then it is *not* a sum of three squares.

(The proof of the converse is omitted.) □

For large n, w note that $1/8$ of all integers are of form $8k + 7$; $1/(8 \cdot 4)$ are of form $4(8k+7)$; $1/(8 \cdot 4^2)$ are of form $4^2(8k+7)$, and so on; each of these is mutually exclusive. So the probability that a randomly chosen integer cannot be expressed as a sum of three squares is

$$\left(\frac{1}{8} + \frac{1}{8 \cdot 4} + \frac{1}{8 \cdot 4^2} + \cdots\right) = \frac{1}{8}\left(1 + \frac{1}{4} + \frac{1}{4^2} + \cdots\right) = \frac{1}{8}\frac{4}{3} = \frac{1}{6}$$

and this probability does not depend on the magnitude of n.

We will now prove Lagrange's four-square theorem, given the following:

Theorem 4. *([**7**, p.315]; Minkowski) Let A be a nonsingular real n by n matrix, and let Λ be the lattice of integer linear combinations of the columns of A. If $\mathcal{C}$ is a set in $\mathbb{R}^n$ which is convex and symmetric about $\vec{0}$, and if $v(\mathcal{C}) > 2^n \det(A)$, then there is a lattice point $\vec{x} \in \Lambda$ such that $\vec{x} \neq 0$ and $\vec{x} \in \mathcal{C}$.*

This result is sometimes known as Minkowski's convex body theorem for general lattices.

Theorem 5. *([**7**, p.317]; originally due to Lagrange) All positive integers can be expressed as sums of four squares.*

Proof: First, we note from the previous discussion that this is the best possible bound. And we have a product property as in (3-1) for sums of two squares, because of the identity

$$\begin{aligned} & (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ = \; & (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ + \; & (x_1y_2 - x_2y_4 - x_3y_1 + x_4y_2)^2 + (x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1)^2 \end{aligned} \tag{3-2}$$

so if m and n can be written as sums of four squares, so can mn. So it is enough to show that all primes can be expressed as sums of four squares.

Let Λ be the lattice of integer linear combinations of $(p, 0, 0, 0), (0, p, 0, 0), (r, s, 1, 0), (s, -r, 0, 1)$, where r, s are chosen so that $r^2 + s^2 + 1 \equiv 0 \pmod p$. (The existence of such r, s is a standard result in the theory of quadratic forms; see for example [**7**, Thm. 5.14].) Then we take

$$A = \begin{bmatrix} p & 0 & r & s \\ 0 & p & s & -r \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

and we can write any point $\vec{x}$ in Λ as $A\vec{t}$ for some $\vec{t} \in \mathbb{Z}^4$. Then we have

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= (pt_1 + rt_3 + st_4)^2 + (pt_2 + st_3 - rt_4)^2 + t_3^2 + t_4^2 \\ &\equiv (1 + r^2 + s^2)(t_3^2 + t_4^2) \pmod{p} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

Now, the volume of a single cells in the lattice Λ is given by the determinant of A, which is p^2. Let $\mathcal{C}$ be the ball of radius $\sqrt{2p}$ centered on the origin; this has volume $2\pi^2 p^2$. So by the previous theorem of Minkowski, there is a point $\vec{x} = (x_1, x_2, x_3, x_4)$ such that $\vec{x} \neq \vec{0}$ and $\vec{x} \in \mathcal{C}$. Then $0 < x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2p$, and $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{p}$, so we conclude that $x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$.

□

Finally, since

$$169 = 13^2 = 12^2 + 5^2 = 12^2 + 4^2 + 3^2 = 10^2 + 8^2 + 2^2 + 1^2 = 8^2 + 8^2 + 6^2 + 2^2 + 1^2$$

gives representations of 169 as the sum of one, two, three, four, and five *positive* squares, we see that we can write any integer $n \geq 169$ as a sum of five positive squares. We simply write $n - 169$ as a sum of k positive squares, $0 \leq k \leq 4$ (this can be done since n is a sum of four squares, some of which may be zero), and to this sum append the representation of 169 as $5 - k$ positive squares.

4. Waring's problem. Edward Waring, in his 1770 book *Meditationes Algebraicae*, asked a question which is usually interpreted as: for any positive integer k, does there exist an integer $g(k)$ such that every positive integer can be expressed as a sum of $g(k)$ kth powers, where $g(k)$ depends only on k? We define $g(k)$ in this way, and $G(k)$ as the largest number for which infinitely many numbers require $G(k)$ kth powers to be additively represented. Lagrange's four-square theorem gives $g(k) = 4$; $G(k) = 4$ also, since there are infinitely many numbers which cannot be expressed as a sum of three squares.

It is easy to find a lower bound for $g(k)$ as follows.

Theorem 6. *([**2**, p.11]) For positive integer k,*

$$g(k) \geq [(3/2)^k] + 2^k - 2$$

where $[x]$ is the greatest integer less than or equal to x.

Proof: Consider $n = 2^k[(3/2)^k] - 1$ as a sum of kth powers. Clearly $n < 3^k$, so any expansion of it into kth powers must consist of only copies of 1^k and 2^k. Maximizing the number of 2^k used minimizes the total number of kth powers needed; thus we write

$$n = 2^k([(3/2)^k] - 1) + 1^k(2^k - 1)$$

to minimize the number of kth powers needed; this is

$$([(3/2)^k] - 1) + (2^k - 1) = [(3/2)^k] + 2^k - 2$$

which gives a lower bound for $g(k)$. □

For small k, this gives $g(1) \geq 1$ ($g(1) = 1$ trivially), $g(2) \geq 4$ ($g(2) = 4$ by the four-square theorem), $g(3) \geq 9$, $g(4) \geq 19$; $g(5) = 37$; and so on. Waring made the assertion that $g(2) = 4, g(3) = 9, g(4) = 19$ with only numerical evidence; as far as is known he did not make conjectures about $g(k)$ for $k \geq 5$, although certainly this bound would have been within his reach. Examples of numbers which require $g(k)$ kth powers are

$$7 = 2^2 + 3 \cdot 1^2, 23 = 2 \cdot 2^3 + 7 \cdot 1^3, 79 = 4 \cdot 2^4 + 15 \cdot 1^4, \cdots$$

It is known that the previous theorem gives $g(k)$ exactly in all but finitely many cases.

Theorem 7. *([**2**, p.23]; Dickson-Pillai-Rubugunday-Niven) If $k \geq 6$ and if the following inequality holds:*

$$3^k - 2^k + 2 < (2^k - 1)[(3/2)^k] \tag{4-1}$$

then $g(k) = [(3/2)^k] + 2^k - 2$. However, if

$$3^k - 2^k + 2 \geq (2^k - 1)[(3/2)^k]$$

then we define $N(k)$ by $N(k) = [(3/2)^k] \cdots [(4/3)^k] + [(3/2)^k] + [(4/3)^k]$ and the conclusion is now

$$g(k) = [(3/2)^k] + [(4/3)^k] + 2^k - 3$$

if $2^k < N(k)$, or

$$g(k) = [(3/2)^k] + [(4/3)^k] + 2^k - 2$$

if $2^k = N(k)$.

It has been verified that (4-1) holds for $6 \leq k \leq 200,000$. It is conjectured that it holds for all $k \geq 6$, and a nonconstructive proof exists that there are most only finitely many values of k for which (4-1) does not hold.

It is also of interest to calculate $G(k)$. It is believed that $G(3) = 6$ – that is, that all sufficiently large integers can be written as a sum of at most *six* cubes – and it is proven that $G(3) \leq 7$. It has been proven that only two numbers requires nine cubes [**11**]:

$$23 = 2 \cdot 2^3 + 7 \cdot 1^3, 239 = 2 \cdot 4^3 + 4 \cdot 3^3 + 3 \cdot 1^3$$

and it is believed that $454 = 7^3 + 4 \cdot 3^3 + 3 \cdot 1^3$ is the largest of the numbers requiring eight cubes (fifteen such are known) and $8042 = 16^3 + 12^3 + 2 \cdot 10^3 + 6^3 + 2 \cdot 1^3$ is the largest of those (121 known) requiring seven cubes. Perhaps even $G(3) = 5$. [**14**]

We can also attempt Waring's problem with mixed signs. We say that n is expressible as a *sum and difference* of m kth powers if there exist $x_1, x_2, \cdot, x_m$ integers such that n can be written in the form

$$n = \pm x_1^k + \pm x_2^k + \cdots + \pm x_m^k$$

. How many kth powers do we need in order to express any number as a sum or difference of kth powers? We call this number $w(k)$. Similarly, we define $W(k)$ as the smallest number such that there are infinitely many integers requiring $W(k)$ kth powers to be expressed as a sum and difference. The determination of $w(k)$ and $W(k)$ is conventionally called the "easier" Waring problem, but it is actually more difficult.

Proposition 8. *All positive integers can be expressed as a sum or difference of three squares, that is, $w(2) = 3$*

Proof: We note that all odd numbers can be expressed as a difference of two squares:

$$2x + 1 = (x + 1)^2 - x^2$$

and all even numbers can be expressed as a sum and difference of three squares:

$$2x = x^2 - (x - 1)^2 + 1^2.$$

So $w(2) \leq 3$. But the number 6 cannot be expressed as a sum or difference of two squares; it is not a sum of two squares, by inspection, and by enumeration of cases modulo 4 we see that no integer congruent to 2 modulo 4 is a difference of two squares. So $w(2) = 3$. □

Proposition 9. *All positive integers can be expressed as a sum and difference of at most five cubes, and infinitely many require at least four cubes; that is,*

$$4 \leq W(3) \leq w(3) \leq 5$$

Proof: To find $w(3)$, we begin by noting the following identity:

$$6x = (x + 1)^3 + (x - 1)^3 - 2x^3 \tag{4-2}$$

and from (4-2) we can readily derive the identities

$$\begin{aligned} 6x \pm 1 &= (x + 1)^3 + (x - 1)^3 - 2x^3 \pm 1^3 \\ 6x \pm 2 &= x^3 + (x \pm 2)^3 - 2(x \pm 1)^3 \mp 2^3 \\ 6x + 3 &= (x - 3)^3 + (x - 5)^3 - 2(x - 4)^3 + 3^3 \end{aligned}$$

and these give expressions for all integers, broken down according to their residue class modulo 6, as a sum and difference of at most five cubes.

But all cubes are congruent to $0, 1$ or -1 modulo 9, so numbers of the form $9n \pm 4$ cannot be expressed as a sum and difference of less than four cubes. Thus we conclude that

$$4 \leq W(3) \leq w(3) \leq 5$$

and exact values are not known [**1**]. □

We can also calculate uppper bounds for $w(k)$ in a manner analogous to that for $k = 3$. We begin with the following identity:

$$\sum_m (-1)^{k-m} \binom{k-1}{m} (x + m)^k = k! \left(x + \frac{k-1}{2} \right) \tag{4-3}$$

which gives a representation of $k!(x + (k - 1)/2)$ as a sum and difference of 2^{k-1} kth powers. Proceeding from (4-3), we can find representations of all integers as sums os kth powers. For $k = 4$, for example, this represents $24x + 36$ as a sum and difference of eight fourth powers. Now, we note that the fourth power residues and their negatives modulo 24 are $0, \pm 1, \pm 8, \pm 9$; we need to add at most four of these to get a representative of any residue class modulo 24. Thus, we have a complete residue system modulo 24 where each element is a sum and difference of at most four fourth powers. Combining this with our representation of all integers congruent to 12 modulo 24 in eight fourth powers, we see that $w(4) \leq 12$.

Proposition 10. *All positive integers can be expressed as a sum and difference of at most eighteen fifth powers; that is,* $w(5) \leq 18$.

Proof: Using (4-3) for $k = 5$, we can represent all numbers of form $120x + 240$ – or, equivalently, of form $120x$ – as sums and differences of sixteen fifth powers. Now, if n is odd, then:

Claim 11. *For all odd integers* n, $120|n^5 - n$.

Proof: Factor $n^5 - n = n(n-1)(n+1)(n^2+1)$. Working modulo 5, we note that exactly one of these four factors is divisible by 5 for any n, so $5|n^5 - n$ for all n. Similarly, modulo 3, exactly one of $3|n, 3|n-1, 3|n+1$ is true, so $3|n^5 - n$. Finally, since n is odd, $n-1, n+1, n^2+1$ are all even, so $2^3|n^5 - n$. Since $5, 3, 8$ are relatively prime, we conclude $120|n^5 - n$. □

So all odd integers are fifth power residues modulo 120. Therefore all *even* integers, being twice some odd integer, are the sum of two fifth power residues modulo 120. Since all multiples of 120 are sums and differences of at most sixteen fifth powers, we conclude that $w(5) \leq 18$. □

Similar arguments may show that $w(k)$ is only slightly larger than 2^{k-1} for all k; compare $g(k)$ which is slightly larger than 2^k. The added flexibility of taking differences greatly decreases the number of terms needed.

Erdos and Suranyi [**3**] give the following as exercises:

$$w(k) \leq 2^{k-1} + \frac{1}{2}k!$$

where one uses the identity (4-3) (Ex. 7.8.10), and

$$w(k) \leq G(k) + 1$$

(Ex. 7.8.11). The first of these can be seen by adding $\pm(1^k)$ repeatedly to a multiple of k. Adding $\pm(1^k)$ and $\pm(2^k)$ reduces this bound to

$$w(k) \leq 2^{k-1} + \left\lceil \frac{k!}{2^{k+1}} \right\rceil + (2^k - 1)$$

but this is not much of an improvement, since the second term still dominates. I conjecture that this method can lead to a bound that is exponential in k, particularly some constant times 2^k. However, the best known bound on $G(k)$ is due to Vaughan [**3**, p. 217]

$$G(k) < k(3 \log k + 4.2)$$

so seeking a bound on the order of 2^k is immaterial.

5. The taxicab problem. There is a famous story in the mathematical folklore concerning the preternaturally brilliant[1] Indian mathematician Ramanujan. When Ramanujan was at Cambridge working with Hardy, he took ill and had to be admitted

[1]Due to certain fortuitous properties of the decimal number system, Ramanujan's recognition of 1729 is not as impressive as it may seem at first glance. Ramanujan's observation amounts to seeing that $729 + 1000 = 1728 + 1$, and neither of these additions is particularly hard. Perhaps noting that this is the *least* number with this property is more interesting. This is not meant to belittle Ramanujan – but his true greatness lie elsewhere.

to a hospital. Hardy came to visit him, and remarked that he came in taxicab number 1729, which he found to be a dull number. Ramanujan is said to have responded that this was actually a quite interesting number – it is the smallest number which can be expressed as the sum of two (positive) cubes in two different ways. As a result, the "taxicab numbers"[2] are often defined as those n for which there are solutions in positive integers to the equation

$$n = x^3 + y^3 = u^3 + v^3. \tag{5-1}$$

for which $\{x, y\} \neq \{u, v\}$.

Probabilistically, we can make a heuristic estimate of the density of the taxicab numbers as follows. The number of lattice points in the first quadrant with $x^3 + y^3 \leq n, x \leq y$ is for large n proportional to $n^{2/3}$; call it $kn^{2/3}$, where

$$k = \frac{1}{2}\int_0^1 (1 - x^3)^{1/3} = \frac{\pi^2}{9\Gamma(2/3)^3} = .4416596881...$$

and differentiating this, the expected number of lattice points with $n - 1/2 \leq x^3 + y^3 < n + 1/2$ (and thus $x^3 + y^3 = n$) is about $\frac{2}{3}kn^{-1/3}$. The probability that *two* lattice points are in this strip can be given by standard techniques in probability, using the Poisson distribution; this gives a rough lower bound for the density of the taxicab numbers, rought because it fails to include any number-theoretic information that would make "collisions" more likely. See [**6**] for further information.

There are various methods of finding solutions to (5-1). The first ([**9**, Sec. 5.2]) is by factoring $x^3 + y^3 = n$ to give

$$(x + y)(X^2 - xy + y^2) = B$$

and then trying all possible integer factorizations $n = AB$, where

$$x + y = A, x^2 - xy + y^2 = B$$

from which we get

$$x = \frac{3A \pm \sqrt{12B - 3A^2}}{6}$$

and so for each A we can check if this gives an integer x. For $n = 1729$, $(A, B) = (13, 133)$ and $(19, 91)$ give the two integer solutions to $x^3 + y^3 = n$ and thus a solution to 5-1.

This is of course rather impractical if one wishes to generate a large number of solutions. One method to find solutions is to generate all sums of cubes up to a certain number and see which are equal; this is the method of Lugo and Larsen [**6**]. Another is the "chord-and-tangent" method commonly used in Diophantine analysis. If we have

$$x_1^3 + y_1^3 = u_1^3 + v_1^3$$

and

$$x_2^3 + y_2^3 = u_2^3 + v_2^3$$

[2]Some authors say that the nth taxicab numjber is the smallest number which can be represented in n ways as a sum of two cubes; this seqence begins $(2, 1729, 87539319, 6963472309248, 48988659276962496, \cdots)$ ([**10**, A011541]; the sixth term is unknown) and is much sparser than the sequence of taxicab numbers under our definition.

then we note that $x^3 + y^3 = u^3 + v^3$ is a curve of degree three in four dimensions, and thus it has three intersections with any line. In particular, it has three intersections with the line through (x_1, y_1, u_1, v_1) and (x_2, y_2, u_2, v_2). We can parametrize this line as

$$(x, y, u, v) = (x_1 + (x_2 - x_1)t, y_1 + (y_2 - y_1)t, u_1 + (u_2 - u_1)t, v_1 + (v_2 - v_1)t)$$

and substituting these into (5-1) gives a cubic in t with integer coefficients. The sum of its roots must be rational, and we know two rational roots $t = 0, t = 1$, so the third root is rational. This gives a third intersection of the line and the curve with rational coefficients; since the taxicab equation is homogeneous, clearing the denominators gives a solution in integers.

However, this solution does not always give a taxicab number; for example, the first two taxicab numbers are

$$1729 = 1^3 + 12^3 = 9^3 + 10^3, 4104 = 2^3 + 16^3 = 9^3 + 15^3$$

but the cubic

$$(1 + t)^3 + (12 + 4t)^3 = 9^3 + (10 + 5t)^3$$

has roots $t = 0, 1, -77/20$, and subtituting $t = -77/20$ and clearing denominators gives

$$(-57)^3 + (-68)^3 = 180^3 + (-185)^3$$

which is not a solution to (5-1) in positive integers. (However, we can rearrange it to get $185^3 = 57^3 + 68^3 + 180^3$; thus this problem is, not surprisingly, essentially the same problem as expressing a cube as a sum of three cubes.) However, noting that

$$20683 = 10^3 + 27^3 = 19^3 + 24^3$$

in conjunction with the above expression for 4104, we get the cubic

$$(2 + 8t)^3 + (16 + 11t)^3 = (9 + 10t)^3 + (15 + 9t)^3$$

which has roots $0, 1, 13/38$; substituting $t = 13/38$ and clearing denominators gives

$$429396751 = 180^3 + 751^3 = 472^3 + 687^3.$$

However, this method tends to generate very large solutions, relying as it does on the clearing of denominators in rational solutions, and there are other methods.

Ramanujan gave two general solutions to (5-1) (see [**15**]). The first is

$$(\alpha + \lambda^2\gamma)^3 + (\lambda\beta + \gamma)^3 = (\lambda\alpha + \gamma)^3 + (\beta + \lambda^2\gamma)^3$$

where

$$\alpha^2 + \alpha\beta + \beta^2 = 3\lambda\gamma^2. \tag{5-2}$$

In general this still suffers from the problem of clearing denominators - we can pick α, β, γ integers and there is no guarantee that $\lambda = (\alpha^2 + \alpha\beta + \beta^2)/3\gamma^2$ is an integer. Alternatively, we can look for integer solutions to (5-2), but this may be quite difficult. Ramanujan's other solution, which does not have these defects, is

$$(A^2 + 7AB - 9B^2)^3 + (2A^2 - 4AB + 12B^2)^3 = (2A^2 + 10B^2)^3 + (A^2 - 9AB - B^2)^3.$$

.

Bounds can be placed on the number of solutions to $x^3+y^3=m$ based on the prime factorization of m, and on the absolute value of x, y (which can be negative) based on m. By observing that any solution satisfies

$$x+y=A, x^2-xy+y^2=B$$

where $AB=m$, we have

$$m \geq B = |x^2-xy+y^2| = \frac{3}{4}x^2 + \left(\frac{1}{2}x-y\right)^2 \geq \frac{3}{4}x^2$$

so $|x| \leq 2\sqrt{m/3}$, and similarly for y. [**9**, p. 149] Also, $x^3+y^3=m$ has no more than $\tau(m)$ solutions in pairs of integers (x,y), where $\tau(m)$ is the number of positive divisors of m. Here (u,v) and (v,u) are counted as distinct solutions if $u \neq v$, so in fact we have $\tau(m)/2$ distinct solutions in the previous sense, unless m is twice a cube in which case our bound is $(\tau(m)+1)/2$. [**9**, p. 177]

6. Further questions and methods. The machinery of generating functions can be brought to bear on this problem. Following the example of Hardy and Littlewood [**12**, p. 3], we can let $\mathcal{A}=(a_m)$ be a strictly increasing sequence of nonnegative integers, and consider the generating function

$$F(z)=\sum_{m=1}^{\infty} z^{a_m}$$

which is convergent in $|z|<1$ since it is a subsequence of the geometric series. We then have

$$F(z)^s = \sum_{m_1=1}^{\infty} \cdots \sum_{m_s=1}^{\infty} z^{a_{m_1}+\cdots+a_{m_s}} = \sum_{n=0}^{\infty} R_s(n) z^n$$

where $R_s(n)$ is the number of representations of n as the sum of s members of $\mathcal{A}$. Various papers of Hardy, Ramanujan, Littlewood, and Vinogradov develop this method using intricate tools from complex analysis. For a trivial example, we can ask in how many ways a number can be written as a sum of, say, two odd numbers. If $\mathcal{A}=(1,3,5,\cdots)$ then we have $F(z)=z/(1-z^2)$. We note that

$$\frac{1}{1-z} = 1+z+z^2+\cdots$$

and differentiating as a formal power series,

$$\frac{1}{(1-z)^2} = 1+2z+3z^2+\cdots$$

and multiplying by z,

$$\frac{z}{(1-z)^2} = z+2z^2+3z^3+\cdots$$

and substituting z^2 for z gives

$$F(z)^2 = \frac{z^2}{(1-z^2)^2} = z^2+2z^4+3z^6+\cdots$$

and so we see that an odd number cannot be written as a sum of two odd numbers, while an even number can be expressed as a sum of two odd numbers in k ways. Of course, there are more direct ways to prove this – but the so-called Hardy-Littlewood method often works when there is no other way.

Although Waring's problem is essentially solved, the so-called "easier" Waring problem – that allowing sums and difference of powers, finding $w(k)$ or $W(k)$ – is still open, as is the "infinite" Waring problem of finding $G(k)$. The only known values of $G(k)$ are $G(2) = 4$ and $G(4) = 16$. Various other generalizations of Waring's problem have been suggested – instead of taking sums of kth powers, one could take sums of values of some polynomial $F(m)$ with integer values evaluated at some integer m. For example, if $F(m) = m(m+1)/2$ we reproduce Fermat's conjecture that any number is a sum of three triangular numbers. Fermat also conjectured that all integers are sums of r r-gonal numbers (three triangular numbers, four squares, and son on); this is an example of a general trend in this area. The denser a sequence of integers, in general, the less such integers we need to express all integers as sums of members of the sequence. If we take the set of primes we get Goldbach's conjecture. And we can take a rather strange generalization due to Scourfield [**8**]: say $2 \leq n_0 \leq n_1 \leq n_2 \leq \cdots$ is a nondecreasing sequence of integers. Then it is true that for each j we can find $r(j)$ such that every sufficiently large number can be written in the form

$$x_j^{n_0} + x_{j+1}^{n_1} + \cdots + x_{j+r}^{n_r}$$

if and only if $\sum_i 1/n_i$ diverges!

References

[**1**] Izzet Coskun. Personal communication.

[**2**] W. J. Ellison. "Waring's Problem". *The American Mathematical Monthly* 78 (1971), 10-36.

[**3**] Paul Erdos and Janos Suranyi. *Topics in the Theory of Numbers.*, 2nd ed. New York: Springer-Verlag, 2002.

[**4**] Euclid. *The Elements.*

[**5**] Emil Grosswald. *Representations of Integers as Sums of Squares.* New York: Springer-Verlag, 1985.

[**6**] Isabel Lugo, Kim Larsen. "Sums of Like Powers". Unpublished manuscript, 2004.

[**7**] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*, 5th ed. New York?: Wiley, 1991.

[**8**] E. J. Scourfield, "A generalization of Waring's problem", *J. London Math. Soc.* 35 (1860) 98-116.

[**9**] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves.* New York: Springer, 1992.

[**10**] Neil J. A. Sloane. *The On-Line Encyclopedia of Integer Sequences.* `http://www.research.att.com/~njas/sequences/`.

[**11**] Charles Small. "Waring's Problem". *Mathematics Magazine* 50 (1977), 12-16.

[**12**] R. C. Vaughan. *The Hardy-Littlewood Method.* London: Cambridge UP, 1981.

[**13**] Eric W. Weisstein. "Landau-Ramanujan Constant." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/Landau-RamanujanConstant.html

[**14**] Eric W. Weisstein. "Waring's Problem." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/WaringsProblem.html

[**15**] Eric W. Weisstein. "Diophantine Equation–3rd Powers." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/DiophantineEquation3rdPowers.html