Some algebraic contributions to Waring's problem

JOINT
MATHEMATICS
MEETINGS

BALTIMORE • JAN 16–19, 2019

AMERICAN MATHEMATICAL SOCIETY
MATHEMATICAL ASSOCIATION OF AMERICA

Paul Pollack

AMS Special Session on
Analytic Number Theory

January 18, 2018

Everyone loves a good origin story

> *Every integer is a square or the sum of two, three, or four squares; every integer is a cube or the sum of two, three, ... nine cubes; every integer is also the square of a square, or the sum of up to nineteen such; and so forth. — E. Waring*

. . . and so forth?

Conjecture (Waring, 1770)

For every integer $k \geq 2$, there is a positive integer $g(k)$ such that every nonnegative integer is the sum of $g(k)$ kth powers of nonnegative integers.

First proof by Hilbert in 1909.

In 1920, Hardy and Littlewood gave a new solution to Waring's conjecture, developing a method Hardy and Ramanujan had utilized a few years before in their study of the partition function — what is now known as the **circle method**.

Almost all subsequent work on Waring's problem goes through the circle method, and for good reason. The method does much more than prove Waring's conjecture. For large s ($s > s_0(k)$), it gives an asymptotic formula for the number of representations as sums of kth powers. And the method applies to many other problems than Waring's.

This program continues to yield fruit, with several new results coming out of groundbreaking work of Wooley, Bourgain, Demeter, Guth and others in just the past few years.

This talk is not about any of that.

Rather, my goal is to make the case that approaches other than the circle method — in which algebra plays a more central role — can shed light on Waring-type problems.

This talk is largely a collection of examples. I warn the experts that much of the first part of the talk is old hat. I will also confess that there is not a satisfying unifying framework for these examples – but maybe someone in the audience can get us closer to that.

Notation

Let R be a semiring (not necessarily commutative). For each $m, s \in \mathbb{Z}^+$, let

$$R_m[s] = \left\{ \sum_{i=1}^{s} \alpha_i^m : \alpha_i \in R \right\}.$$

Since $0 \in R$, we have $R_m[s] \subset R_m[s+1]$. We let

$$R_m[\infty] = \bigcup_{s \geq 0} R_m[s].$$

We say Waring's conjecture holds for mth powers in R if there is a positive integer g with

$$R_m[g] = R_m[\infty].$$

An ‘easy’ example

The classical Waring problem has $R = \mathbb{Z}_{\geq 0}$, and $m \geq 1$ arbitrary.

There is no easy proof of the Waring–Hilbert theorem. However, it *is* easy to prove that Waring's conjecture for mth powers holds in $R = \mathbb{Z}$ when m is *odd*.

I give the proof for $m = 3$; the other cases are similar.

For any $f(x) \in \mathbb{Z}[x]$, define $\Delta f(x) = f(x+1) - f(x)$ (forward difference operator). It is clear that if $f(x) \neq 0$, say with leading term ax^n, then $\Delta f(x)$ has leading term nax^{n-1}.

Now take $f(x) = x^3$. Then $\Delta f(x)$ has leading term $3x^2$, and $\Delta^2 f(x)$ has leading term $6x$.

Hence, $\Delta^2 f(x) = 6x + D$, for some integer D.

(It is easy to compute that $D = 6$, but we won't need this.) On the other hand,

$$\Delta x^3 = (x+1)^3 - x^3,$$

$$\Delta^2 x^3 = (x+2)^3 - (x+1)^3 - (x+1)^3 + x^3.$$

Since 3 is odd, this can be rewritten as

$$\Delta^2 x^3 = (x+2)^3 + (-(x+1))^3 + (-(x+1))^3 + x^3.$$

Comparing the two expressions for $\Delta^2 f(x)$, we conclude that every integer $\equiv D \pmod 6$ is a sum of four cubes in $\mathbb{Z}$.

Using this, we show that every integer is a sum of at most five cubes.

Every integer is a cube mod 6 (in fact, the cube of itself). So given n, we may choose an integer m with $n - m^3 \equiv D \pmod{6}$. Then $n - m^3 = a^3 + b^3 + c^3 + d^3$ for some a, b, c, d, and so

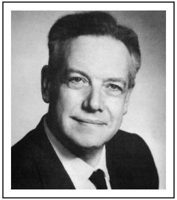
$$n = a^3 + b^3 + c^3 + d^3 + m^3.$$

Open problem: Is every integer the sum of 4 cubes?
If so, then '4' is best possible, since integers $\equiv \pm 4$ mod 9 require at least four cubes.

Developing our above argument further one finds that for **every** positive integer m, there is a positive integer $v(m)$ such that every integer is the sum *or difference* of $v(m)$ mth powers. Using $v(m)$ now for the smallest such integer, we are asking whether $v(3) = 4$ or $v(3) = 5$.

E.M. Wright published this (and more, which I am omitting) in a 1934 paper. He called this modified Waring problem, where one allows differences as well as sums, the "easier Waring problem."

Well, life is full of regrets. Nearly 50 years later (1979), Wright had this to say:



> So far from being "easier" (as I absurdly named it in [8]), the determination of $v(k)$ has turned out to be substantially more difficult than that of $g(k)$, ...

In fact, while $g(k)$ is now known for all but finitely many k, we do not know the value of $v(k)$ for any k other than $k = 2$.

Exercise: $v(2) = 3$.

Waring's problem for $R = \mathbb{C}[T]$

Let m be any positive integer, and let $f(x) = x^m$. Computing $\Delta^{m-1}f(x)$ in the two ways we did for $m = 3$, we obtain a polynomial identity

$$m!x + D_m = (x + m - 1)^m + c_1(x + (m - 2))^m + \cdots + c_{m-1}x^m,$$

where D_m and the c_i are integers.

Suppose we are given any polynomial in $\mathbb{C}[T]$, say $g(T)$. We may choose $x = x(T) \in \mathbb{C}[T]$ to make $m!x + D_m = g(T)$. The above identity shows that $g(T)$ is a sum of m mth powers in $\mathbb{C}[T]$.

Thus, Waring's conjecture holds for $R = \mathbb{C}[T]$ and any $m \geq 1$.

So m mth powers suffice in $\mathbb{C}[T]$. Can one get by with fewer?

Conjecture (Newman and Slater, 1979)

NO!

Heilbronn conjectured that T cannot be written as the sum of fewer than m mth powers of entire functions of the complex variable T.

Theorem (ibid.)

The minimal number of mth powers needed to represent all elements of $\mathbb{C}[T]$ is $> m^{1/2}$, for all integers $m \geq 2$.

Their proof uses an argument with Wronskians, similar to one proof of the polynomial abc-theorem (Mason–Stothers).

One can also look at polynomials over rings other than $\mathbb{C}$.

Let F be a finite field. If the characteristic of F is larger than m, the argument on the last slide suffices to show that Waring's conjecture holds for the mth powers in $F[T]$.

In fact, the restriction on the characteristic is not necessary. This is a 1933 theorem of Paley — better known for his contributions to analysis.

Theorem (Paley, 1933)

For any finite field F, and any positive integer m, Waring's conjecture for mth powers holds in $F[T]$.

Note: The set of elements representable need **not** be all of $F[T]$!

For the proof, Paley first finds polynomials $G(T), H(T) \in F$ with the property that

$$G(T)x + H(T)$$

is identically a sum of mth powers in $F[T][x]$.

As an immediate consequence, every polynomial congruent to $H(T)$ modulo $G(T)$ is expressible as the sum of a bounded number mth powers in $F[T]$. It is then elementary to deduce Waring's conjecture, and that for all large s, the polynomials expressible as sums of mth powers are exactly those polynomials that are sums of mth powers modulo $G(T)$.

To produce $G(T), H(T)$, Paley relies on the following pretty lemma:

Lemma

Let F be a finite field of order $q = p^h$, where p is prime. Let m be a positive integer, and write m in base p:

$$m = p^{n_1} + p^{n_2} + \cdots + p^{n_k},$$

where none of $n_1, n_2, \ldots$ occur more than $p-1$ times. (So k is the sum of the base p digits of m.) For every integer k' with $h(p-1)k' > k$, we have

$$\sum_{\substack{g(x) \in F[x] \\ g \text{ monic} \\ \deg g(x) = k'}} g(x)^m = 0.$$

The minimal number of *m*th powers needed has been studied recently by Vaserstein, and Liu and Wooley.

Several other attractive “Waring problems” could be exhibited. I would be remiss if I neglected to mention Hilbert’s original proof of Waring’s original problem. This has a definite algbraic flair, relying on certain complicated polynomial identities. Using these identities, Ellison has shown that if K is any non-real field (meaning -1 is a sum of squares) of characteristic 0, then Waring’s problem is true for the *m*th powers in K, for all m.

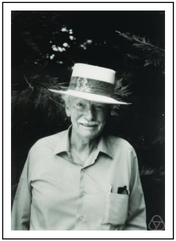
It should also be mentioned that Vaserstein has proved very general results for a large class of commutative rings. For example, if R is any finitely generated commutative ring, and m is any prime, then Waring’s conjecture holds for *m*th powers in R.

Waring's problem for integral quaternions

Let $\mathbb{L}$ be the ring of Lipschitz integral quaternions — those quaternions of the form

$$a + bi + cj + dk,$$

where all of $a, b, c, d \in \mathbb{Z}$.



Theorem (Niven, 1946)

Waring's problem is true for squares in $\mathbb{L}$. The elements representable as sums of squares are precisely those with b, c, d even. Moreover, for all these elements, three squares suffice (and this is sharp).

Theorem (P.)

Let m be an integer with $m > 2$, and suppose $2^r \parallel m$. If $r = 0$ (i.e., m is odd), then all integral quaternions are sums of mth powers, while if $r > 0$, then the integral quaternions that are sums of mth powers are precisely those for which $2^r \mid b, c, d$ and $2^{r+1} \mid b + c + d$. Moreover, all of these are expressible as a sum of $g_{\mathbb{L}}(m)$ mth powers, where $g_{\mathbb{L}}(m)$ is a positive integer depending only on m.

The general strategy of the proof is along the same lines as Paley's. One uses various identities to show there is a positive integer G such that all elements in a certain congruence class mod G are expressible as the sum of a bounded number of of mth powers in $\mathbb{L}$.

This more or less gives the theorem, while simultaneously showing that the representable elements are those that are representable as sums of mth powers mod G.

To determine which elements of $\mathbb{L}$ are sums of mth powers mod G, one factors G into prime powers. For an odd prime power p^k, one has that $\mathbb{L}/(p^k) \cong M_2(\mathbb{Z}/p^k)$, and it is easy to see that everything in the latter ring is a sum of mth powers. For the power of 2 in G, I have only an ad hoc argument at the moment.

How many mth powers do we need?

The number of such mth powers can be bounded in terms of the numbers $g(m)$ and $G(m)$ that appear in the classical Waring problem. This gives an upper bound of $O(m \log m)$.

It would seem an attractive question which I don't know the answer to is to get a "reasonable" lower bound on the number of required mth powers.

$+\,\mathrm{h}\,\{a_n\}^k \quad \varphi \circ \cup$