A Walk through Waring's Problem

Garo Sarajian

University of California, Santa Barbara

May 22nd, 2018

Outline

Outline

Introduction

Notation:

- Given a real function $g(x)$ and a function $f(x)$, we have $f(x) = O(g(x))$ means that there exists a constant C independent of x such that $|f(x)| \leq Cg(x)$ for all x.
- We'll also use $\ll$ and $\gg$, where $f(x) \ll g(x)$ is equivalent to $f(x) = O(g(x))$.
- $f(x) \sim g(x)$ means $f(x)/g(x) \to 1$ as $x \to \infty$.
- $f(x) = o(g(x))$ means $f(x)/g(x) \to 0$ as $x \to \infty$

History

- In 1621, C. G. Bachet claimed without proof that every natural number is a sum of four squares. It wasn't until 1770 until Lagrange provided a proof of this theorem.

- In 1770, Edward Waring wrote that every natural number is a sum of 9 nonnegative cubes, and 19 fourth powers, and so on. This is the genesis of Waring's Problem, which concerns writing natural numbers as sums of kth powers.

- The original problem focused on being able to write all natural numbers as a sum of kth powers. We denote $g(k)$ as the smallest number such that every natural number is the sum of $g(k)$ nonnegative kth powers.

History: Examples

- (Squares) Since 7 can't be written as a sum of three squares, Lagrange's Theorem implies $g(2) = 4$.
- (Cubes): 23 requires 9 cubes, so $g(3) \geq 9$.
- (Fourth powers): 79 requires 19 fourth powers, so $g(4) \geq 19$.

$g(k)$

- In 1909, Hilbert proved the existence of $g(k)$ for all k using combinatorial identities.

- The $g(k)$ are now almost entirely determined, with $g(k) = 2^k + \lfloor (3/2)^k \rfloor - 2$ for all but finitely many k.

- The number $2^k \left(\lfloor (3/2)^k \rfloor\right) - 1$ can only be written with 1^k and 2^k, and $g(k)$ is determined by how many kth powers are needed to represent this number. So $g(2) = 4$, $g(3) = 9$, $g(4) = 19$, etc.

The Modern Problem

- The focus has now turned to finding how many kth powers are needed to represent every sufficiently large number. Denote $G(k)$ as the smallest number such that every sufficiently large natural number is the sum of $G(k)$ nonnegative kth powers.

- Examples (Squares): Since $8n + 7$ requires four squares, $G(2) = 4$.

- (Cubes): In 1909, Dickson proved that 23 and 239 are the only two numbers that require 9 cubes. In 1943, Linnik provide that only finitely many numbers require 8 cubes, so $G(3) \leq 7$. Since $9n + 4$ requires at least four cubes, $G(3) \geq 4$.

- (Fourth powers): In 1939, Davenport proved that $G(4) = 16$. There are only seven numbers that require 19 fourth powers. In total, there are 96 natural numbers that cannot be written as a sum of sixteen 4th powers. 13792 is the largest such number.

Bounds for G(k)

$1 = G(1) = 1$	$g(1) = 1$
$4 = G(2) = 4$	$g(2) = 4$
$4 \leq G(3) \leq 7$	$g(3) = 9$
$16 = G(4) = 16$	$g(4) = 19$
$6 \leq G(5) \leq 17$	$g(5) = 37$
$9 \leq G(6) \leq 24$	$g(6) = 73$
$8 \leq G(7) \leq 31$	$g(7) = 143$
$32 \leq G(8) \leq 39$	$g(8) = 279$
$13 \leq G(9) \leq 47$	$g(9) = 548$
$12 \leq G(10) \leq 55$	$g(10) = 1079$

$12 \leq G(11) \leq 63$	$g(11) = 2132$
$16 \leq G(12) \leq 72$	$g(12) = 4223$
$14 \leq G(13) \leq 81$	$g(13) = 8384$
$15 \leq G(14) \leq 90$	$g(14) = 16673$
$16 \leq G(15) \leq 99$	$g(15) = 33203$
$64 \leq G(16) \leq 108$	$g(16) = 66190$
$18 \leq G(17) \leq 117$	$g(17) = 132055$
$27 \leq G(18) \leq 125$	$g(18) = 263619$
$20 \leq G(19) \leq 134$	$g(19) = 526502$
$25 \leq G(20) \leq 142$	$g(20) = 1051899$

Outline

Circle Method Setup

Let $e(\alpha)$ denote $e^{2\pi i\alpha}$.
Let

$$f_k(\alpha, P) = \sum_{1 \le x \le P} e(\alpha x^k)$$

Then

$$f_k(\alpha, P)^s = \sum_{1 \le x_1, x_2, \dots x_s \le P} e(\alpha(x_1^k + \cdots + x_s^k))$$

$$= \sum_{n=1}^{sP^k} R_{s,k}(n) e(\alpha n)$$

where $R_{s,k}(n)$ is the number of ways we can represent n as a sum of s kth powers.
Thus,

$$R_{s,k}(n) = \int_0^1 f_k(\alpha, P)^s e(-n\alpha) d\alpha$$

Major and Minor Arcs

-To evaluate the integral, split $[0,1]$ into "major" and "minor" arcs:

$$\mathfrak{M}(q,a) = \left\{ \alpha \in [0,1] \mid \left| \alpha - \frac{a}{q} \right| < \frac{1}{qP^{k-1}} \right\}$$

$$\mathfrak{M} = \bigcup_{\substack{1 \le a \le q \le P \\ (a,q)=1}} \mathfrak{M}(q,a)$$

$$\mathfrak{m} = [0,1] \setminus \mathfrak{M}$$

-For $s \ge \max\{5, k+1\}$, Hardy and Littlewood proved:

Theorem

$$\int_{\mathfrak{M}} f_k(\alpha, P)^s \, e(-n\alpha) d\alpha = C(s,k)\mathfrak{S}(n) n^{s/k-1} + o(n^{s/k-1})$$

Major and Minor Arcs

$$\int_{\mathfrak{M}} f_k(\alpha, P)^s \, e(-n\alpha) d\alpha = C(s,k)\mathfrak{S}(n) n^{s/k-1} + o(n^{s/k-1})$$

-Most of the research on Waring's Problem focuses on minimizing the contribution from the minor arcs, and showing that for some s_0,

$$\int_{\mathfrak{m}} f_k(\alpha, P)^{s_0} \, e(-n\alpha) d\alpha = o(n^{s_0/k-1})$$

If the singular series $\mathfrak{S}(n)$ doesn't vanish, these will together imply that $R_{s_0,k}(n) \gg n^{s_0/k-1}$, so in particular, $G(k) \leq s_0$.

Outline

Lower Bounds for $G(k)$

$$R_{s,k}(n) = C(s,k)\mathfrak{S}(n)n^{s/k-1} + o(n^{s/k-1})$$

- $G(k) \geq k+1$.

- For any s, the singular series $\mathfrak{S}(n)$ converges absolutely and is nonnegative. Hardy and Littlewood proved that it is positive for all n if and only if we can solve the corresponding Waring's problem locally:

Theorem

For every $n \in \mathbb{N}$, the singular series $\mathfrak{S}(n)$ is positive if for every $m \in \mathbb{N}$, the equation

$$x_1^k + \cdots + x_s^k = n \mod (m)$$

has a solution with $(x_1, m) = 1$.

The subproblem of $\Gamma(k)$

- Denote $\Gamma(k)$ the smallest value such that for every m, every residue class $\mod m$ has a nontrivial solution.

- It's widely believed that $G(k) = \max\{k+1, \Gamma(k)\}$.

- Hardy and Littlewood computed $\Gamma(k)$ for certain classes of k:

$$\begin{aligned}
\Gamma(2^r) &= 2^{r+2} \\
\Gamma(3 \cdot 2^r) &= 2^{r+2} \\
\Gamma(p^r(p-1)) &= p^{r+1} \\
\Gamma(p^r(p-1)/2) &= (p^{r+1}-1)/2 \\
\Gamma(p-1) &= p \\
\Gamma((p-1)/2) &= (p-1)/2
\end{aligned}$$

Bounds for G(k)

$1 = G(1) = 1$	$g(1) = 1$
$4 = G(2) = 4$	$g(2) = 4$
$4 \leq G(3) \leq 7$	$g(3) = 9$
$16 = G(4) = 16$	$g(4) = 19$
$6 \leq G(5) \leq 17$	$g(5) = 37$
$9 \leq G(6) \leq 24$	$g(6) = 73$
$8 \leq G(7) \leq 31$	$g(7) = 143$
$32 \leq G(8) \leq 39$	$g(8) = 279$
$13 \leq G(9) \leq 47$	$g(9) = 548$
$12 \leq G(10) \leq 55$	$g(10) = 1079$

$12 \leq G(11) \leq 63$	$g(11) = 2132$
$16 \leq G(12) \leq 72$	$g(12) = 4223$
$14 \leq G(13) \leq 81$	$g(13) = 8384$
$15 \leq G(14) \leq 90$	$g(14) = 16673$
$16 \leq G(15) \leq 99$	$g(15) = 33203$
$64 \leq G(16) \leq 108$	$g(16) = 66190$
$18 \leq G(17) \leq 117$	$g(17) = 132055$
$27 \leq G(18) \leq 125$	$g(18) = 263619$
$20 \leq G(19) \leq 134$	$g(19) = 526502$
$25 \leq G(20) \leq 142$	$g(20) = 1051899$

Finding $\Gamma(k)$

- Hardy and Littlewood proved an algorithm for computing $\Gamma(k)$, and computed its values for small k.

- They speculated that for prime k not falling into any of the aforementioned classes, $\Gamma(k)$ is determined by the corresponding Waring's problem $\mod p$, where p is the smallest prime in the arithmetic progression $dk + 1$.

- However, $k = 31$ turns out to be a counterexample to this, and $k = 59$ also.

Outline

Upper Bounds for $G(k)$

$(k-2)2^{k-1}+5$	Hardy & Littlewood (1922)
$(k-2)2^{k-2}+k+5+O(k/\log(k))$	Hardy & Littlewood (1925)
$32(k\log(k))^2$	Vinogradov (1934)
$k^2\log(4)+(2-16)\log(k)$	Vinogradov (1935)
$6k\log(k)+3k\log(6)+4k$	Vinogradov (1935)
$k(3\log(k)+11)$	Vinogradov (1947)
$k(3\log(k)+9)$	Tong (1957)
$k(3\log(k)+5.2)$	Jing-Run Chen (1958)
$2k(\log(k)+2\log(\log(k))+O(\log_3(k)))$	Vinogradov (1959)
$2k(\log(k)+\log(\log(k))+O(1))$	Vaughan (1989)
$k(\log(k)+\log(\log(k))+O(1))$	Wooley (1992)

Bounding Minor Arc Contributions

- When $\alpha \in \mathfrak{m}$, the summands in $f_k(\alpha, P)$ are more equidistributed, so they exhibit more cancellation than the trivial bound $|f_k(\alpha, P)| \leq P$. Weyl proved the following theorem that relates f_k to the size of denominator in α's rational approximation:

Theorem

$$f_k(\alpha, P) \ll P^{1+\epsilon}(q^{-1} + P^{-1} + qP^{-k})^{1/(2^{k-1})}$$

- This is combined with mean value estimates to get the desired bounds for the minor arc contributions:

$$\left| \int_{\mathfrak{m}} f_k\left(\alpha, P\right)^s e(-n\alpha) d\alpha \right| \leq \max_{\alpha \in \mathfrak{m}} \left| f_k(\alpha, P) \right|^{s-2r} \int_0^1 \left| f_k(\alpha, P) \right|^{2r} d\alpha$$

Mean Value Estimates

$$\int_0^1 |f_k(\alpha, P)|^{2r} \, d\alpha$$

Mean Value Estimates

$$\int_0^1 |f_k(\alpha, P)|^{2r}\, d\alpha$$

$$= \int_0^1 f_k(\alpha, P)^r \overline{f_k(\alpha, P)^r} d\alpha$$

Mean Value Estimates

$$\int_0^1 |f_k(\alpha, P)|^{2r}\, d\alpha$$

$$= \int_0^1 f_k(\alpha, P)^r \overline{f_k(\alpha, P)^r} d\alpha$$

$$= \int_0^1 \sum_{1 \le x_j, y_j \le P} e(\alpha(x_1^k + x_2^k + \cdots + x_r^k - y_1^k - \cdots - y_r^k)) d\alpha$$

Mean Value Estimates

$$\int_0^1 |f_k(\alpha, P)|^{2r}\, d\alpha$$

$$= \int_0^1 f_k(\alpha, P)^r \overline{f_k(\alpha, P)^r} d\alpha$$

$$= \int_0^1 \sum_{1 \le x_j, y_j \le P} e(\alpha(x_1^k + x_2^k + \cdots + x_r^k - y_1^k - \cdots - y_r^k)) d\alpha$$

$= \text{The number of integral solutions to } x_1^k + \cdots + x_r^k = y_1^k + \cdots + y_r^k$

with $1 \le x_j, y_j \le P$

Mean Value Estimates

- There are several techniques for bounding these mean values:
- Diminishing Ranges
- p-adic Ranges
- Efficient Differencing with Smooth Numbers

Diminishing Ranges

- Instead of looking at $x_j, y_j \in [1, P]$, we can restrict the ranges that they lie in.

$$\frac{P_j}{2} \leq x_j, y_j \leq P_j \quad \text{where } P_j = \frac{P^{(1-1/k)^{j-1}}}{2^{(j-1)(k-1)}}$$

- Then the only solutions are the diagonal ones, so the number of solutions to the diophantine equation is $\ll \prod_j P_j$
- This gives $G(k) \leq s_0$ for $s_0 \sim Ck\log(k)$ for a positive constant C.

p-adic Ranges

- Similarly, we can look at the p-adic analogue, considering solutions in the form

$$x_1^k + p^k(x_2^k + x_3^k + \cdots) = y_1^k + p^k(y_2^k + y_3^k + \cdots)$$
$$\text{with } p \sim M, x_j, y_j \sim P/M$$

- Then a proportion of the solutions satisfy $x_1^k \equiv y_1^k \mod (p^k)$

Efficient Differencing with Smooth Numbers

- Recall that a R-smooth number is a number whose largest prime factor is $\leq R$. Denote $\mathcal{A}(P, R)$ to be the set of R-smooth numbers in $[1, P]$.

$$x_1^k + \cdots + x_r^k = y_1^k + \cdots + y_r^k$$
$$\text{with } x_j, y_j \in \mathcal{A}(P, R)$$

- If $R \geq P^\eta$ for some fixed η, then $\mathcal{A}(P, R)$ has asymptotic density. After iterating, the related auxiliary equation can be approached with a variety of methods.

New Approaches

- Modify p-adic and efficient differencing approaches by selecting primes in certain arithmetic progressions as the basis for each.

- Apply these new methods in conjunction with methods used in the proof of Vinogradov's Mean Value Theorem to a variant of Hypothesis K.

- G. H. Hardy and J. E. Littlewood. Some Problems of "Partitio Numerorum" (VIII): The Number $\Gamma(k)$ in Waring's Problem. London Mathematical Society, Volume s2-28, Issue 1 (1928), p. 518-542.
- H. Montgomery and R. C. Vaughan, Multiplicative Number Theory: Classical Theory. Cambridge University Press, Cambridge, 2007.
- M. Nathanson. Additive Number Theory: The Classical Bases. Springer-Verlag New York, 1996.
- R. C. Vaughan. The Hardy-Littlewood Method, volume 125 of Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge, New York, 2nd edition, 1997.
- R. C. Vaughan. A New Iterative Method in Waring's Problem. Acta Mathematica, Volume 162 (1992), p. 1-71.
- R. C. Vaughan and T. D. Wooley. Waring's Problem: A Survey. Number Theory for the Millennium. III Natick, MA. (2002), p. 301-340.

- T. D. Wooley. Large Improvements in Waring's Problem. Annals of Mathematics, 135(3) (1992), 131-164.
- T. D. Wooley. On Waring's problem for intermediate powers. Act Arith., 176(3) (2016), 241-247.
- T. D. Wooley. Nested Efficient Congruencing and Relatives of Vinogradov's Mean Value Theorem. Submitted, (2017) 85pp; arxiv:1708.01220.
65 (2) (1997) 325-333.

Thanks!