AN EASY INTRODUCTION TO THE CIRCLE METHOD

EVAN WARNER

This talk will try to sketch out some of the major ideas involved in the Hardy-Littlewood circle method in the context of Waring's problem.

1. Setup

First, let's establish a general setup. We could strive for more generality, but this framework will allow us to discuss many of the problems that fall under the purview of the circle method.

Let A be a subset of the natural numbers $\mathbb{N}$ (here considered so as to exclude zero), and set

$$r(n; s, A) := \#\{\text{ways to write } n \text{ as a sum of } s \text{ elements of } A\}.$$

Many important problems can be phrased in terms of these functions. For example, let $A = \{2, 3, 5, 7, \ldots\}$ be the set of prime numbers. Then

$$\text{ternary Goldbach conjecture} \iff r(n; 3, A) > 0 \text{ for all } n \text{ odd and greater than } 5$$

and

$$\text{binary Goldbach conjecture} \iff r(n; 2, A) > 0 \text{ for all } n \text{ even and greater than } 2.$$

As another example, let $A = \{1, 2^k, 3^k, 4^k, \ldots\}$ be the set of kth powers, where k is an integer ≥ 2. Then, being deliberately vague,

$$\text{Waring's problem} \iff \text{knowledge of } r(n; s, A).$$

There are other problems that can be attacked with the circle method but that don't quite fit into our framework here; for example, determining asymptotics of the partition function $p(n)$ or proving theorems about small gaps in primes. For this talk, we'll concentrate on Waring's problem, as it is of moderate difficulty and illustrates some basic ideas nicely. There will be no effort at complete proofs.

2. Background on Waring's problem

Fix an integer $k \geq 2$ for the remainder of the talk. We're interested in the number of ways of expressing a positive integer as a sum of s kth powers. If A is the set of kth powers, set $r_s(n) := r(n; s, A)$. Waring's original problem was to prove that for all k, there exists an s such that $r_s(n) > 0$ for all $n > 0$. This problem was proven by Hilbert in 1909, using ideas of Hurwitz that predate the circle method.

Of course, refinements immediately present themselves. What is the minimal such s, a quantity usually denoted by $g(k)$? Formulas are now known for $g(k)$, due to various 20th century mathematicians. More interestingly (and more challengingly), one can ask what is the minimum s if we allow finitely many exceptions in n, a quantity denoted by $G(k)$? Here I believe the best known bound is $G(k) \leq$

$k(\log k + \log\log k + 2 + C\log\log k/\log k)$ for some constant C, due to Wooley. It is conjectured that $G(k)$ should be approximately linear in k.

Finally, we can ask for asymptotics for $r_s(n)$. We will examine this problem, following Hardy-Littlewood, for s sufficiently large in terms of k. Specifically, we will require $s \geq 2^k + 1$; the largest range on which the asymptotics we will derive are known to be valid is $s \geq k^2(\log k + \log\log k + C)$ for some constant C, due to Ford. The conjectured range is the considerably stronger $s \geq k + 1$.

3. Generating functions

Our first idea is that generating functions are fun and useful, so let's make a generating function for the characteristic function of our set A. Set

$$F(x) := \sum_{a\in A} x^a = \sum_{j=1}^{\infty} x^{j^k}.$$

Then we see immediately that

$$F(x)^s = \left(\sum_{j=1}^{\infty} x^{j^k}\right)^s = \sum_{n=1}^{\infty} r_s(n)x^n,$$

just by regrouping terms. Thus $F(x)^s$ is the generating function for $r_s(n)$.

Now, to pick out the coefficients, we integrate around a circle (hence the name "circle method"). Let γ be a counterclockwise circle centered at the origin of radius r. Totally ignoring convergence issues for the moment, we calculate that

$$\begin{aligned}\frac{1}{2\pi i}\int_\gamma \frac{F(x)^s}{x^{n+1}}\,dx &= \frac{1}{2\pi i}\int_\gamma \sum_{j=1}^{\infty} r_s(j)x^{j-n-1}\,dx \\ &= \sum_{j=1}^{\infty}\frac{r_s(j)}{2\pi i}\int_\gamma x^{i-n-1}\,dx \\ &= r_s(n),\end{aligned}$$

using the well-known fact from basic complex analysis that $\frac{1}{2\pi i}\int_\gamma x^m\,dx$ is equal to one if $m = -1$ and zero otherwise. This calculation turns out to be valid when $r < 1$. Thus, the problem of finding $r_s(n)$ turns into the evaluation or estimation of the integral $\frac{1}{2\pi i}\int_\gamma \frac{F(x)^s}{x^{n+1}}\,dx$. In fact, this is what Hardy and Littlewood did.

4. Generating functions à la Vinogradov

We are going to do something slightly different, following a technical refinement due to Vinogradov: instead of using a power series generating function and integrating over a circle, we use a trigonometric series and integrate over the line segment $[0, 1]$. Set

$$e(x) := e^{2\pi i x}.$$

Again ignoring convergence issues (this time they're more serious, as what I'm going to write down doesn't actually make very much sense), define

$$f(x) := \sum_{a\in A} e(ax) = \sum_{j=1}^{\infty} e(j^k x).$$

Then, as before, we find that

$$f(x)^s = \left(\sum_{j=1}^{\infty} e(j^k x)\right)^s = \sum_{n=1}^{\infty} r_s(n) e(nx)$$

is the corresponding "trigonometric generating function" for $r_s(n)$. We can easily calculate

$$\begin{aligned}\int_0^1 f(x)^s e(-nx)\,dx &= \int_0^1 \sum_{j=1}^{\infty} r_s(j) e(jx) e(-nx)\,dx \\ &= \sum_{j=1}^{\infty} r_s(j) \int_0^1 e(jx) e(-nx)\,dx \\ &= r_s(n),\end{aligned}$$

where we used that $\int_0^1 e(jx)e(-nx)\,dx$ is equal to one if $n = j$ and zero otherwise.

Now, we introduce in one swoop a simplification and a fix to our convergence issues. Let

$$f_P(x) := \sum_{j=1}^{P} e(j^k x),$$

where P is a finite positive integer. Then

$$f_P(x)^s = \sum_{n=1}^{\infty} r'_s(n) e(nx),$$

where

$$r'_s(n) = \#\{\text{solutions to } x_1^k + \ldots + x_s^k = n \text{ such that } 1 \le x_i \le P \text{ for each } i\}.$$

This is, of course, very much *not* the function we were looking for. But wait! As long as $P \ge \lfloor n^{1/k} \rfloor$ we *do* have $r'_s(n) = r_s(n)$, so in that range $f_P(x) = f(x)$. So to find asymptotics for $r_s(n)$ it suffices to calculate

$$\int_0^1 f_P(x)^s e(-nx)\,dx$$

for $P \ge \lfloor n^{1/k} \rfloor$, and this integral converges nicely.

5. Splitting up into major and minor arcs

To estimate this integral well, let's think a bit about exponential sums. If we have a collection of N "random" numbers on the unit circle and add them up, we expect the sum to be about $\sqrt{N}$ (this is an instance of the "square root law" for random walks). For sufficiently generic $x \in [0,1]$, the collection of numbers $\{e(j^k x)\}_{1 \le j \le P}$ should look fairly random, at least if P is large enough. So for sufficiently generic x, we expect $f_P(x) \sim \sqrt{P}$.

This *can't* be true for all x, however. For example,

$$f_P(0) = \sum_{i=1}^{P} e(i^k \cdot 0) = P,$$

which in particular shows that we can't expect to get anything useful by bounding the integral by $\sup_x |f_P(0)|$. A little experimenting shows that this lack of cancellation occurs fairly often whenever x is very close to a rational number with small denominator – not always, but enough to be worrying. For example, if $k = 2$ then we find $f_P(1/2)$ is actually bounded (excellent cancellation!) but $f_P(1/8) \sim CP$ for some nonzero constant C because squares are biased modulo 8: half the time, they are equal to 1 modulo 8, and a quarter of the time each they are equal to 0 and 4 modulo 8.

Let's formalize this intuition as follows: fix a small $\delta > 0$ (if you prefer a definite value, feel free to take $\delta = 1/100$). Define

$$M_{a,q} = \left\{ x \in \mathbb{R}/\mathbb{Z} : \left| x - \frac{a}{q} \right| < P^{-k+\delta} \right\} \subset \mathbb{R}/\mathbb{Z}.$$

Each of these is a smallish interval around the fraction a/q. We let

$$M = \bigcup_{\substack{1 \le q \le P^\delta \\ 1 \le a \le q, (a,q)=1}} M_{a,q}.$$

This is a union over all $M_{a,q}$ such that a/q is a fraction in $\mathbb{R}/\mathbb{Z}$ with "small" denominator (compared to P).

We'll call M, as a set, the *major arcs*. This is the locus on which we expect little cancellation and therefore expect the bulk of the integral to lie. Let $m = [0,1] - M$ be the complement, the *minor arcs*, for which we do expect some cancellation. This setup is ubiquitous in the context of the circle method.

The goals going forward are the following:

- Evaluate $\int_M f_P(x)^s e(-nx)\, dx$, and
- Show that $\left| \int_m f_P(x)^s e(-nx)\, dx \right|$ is small compared to the above.

6. Major arcs

On the major arcs, $f_P(x)$ is somehow "almost constant." Let's make this precise as follows: let $x \in M_{a,q}$ and write $y = x - \frac{a}{q}$.

Lemma 6.1. *We have*

$$f_P(x) = \frac{1}{q} \sum_{m=1}^{q} e(m^k a/q) \int_0^P e(y\xi^k)\, d\xi + O(P^{2\delta}).$$

Proof (sketch). First, we collect terms i in the same residue class modulo q. If we write

$$i = qj + m, \quad 1 \le m \le q,$$

then

$$f_P(x) = \sum_{m=1}^{q} \left[e(m^k a/q) \sum_{j=1}^{\lfloor P/q \rfloor} e(y(qj+m)^k) \right].$$

The inner sum is almost equal to the integral

$$\frac{1}{q} \int_0^P e(y\xi^k)\, d\xi$$

by replacing j by a continuous variable η and setting $\xi = q\eta + m$. The error is crudely estimated to be $O(P^{2\delta})$ is crudely estimated by calculating the derivative. □

When we plug in the above lemma to the integral over the major arcs and crudely estimate (the steps are not difficult and also not enlightening), we get the following result:

$$\int_M f_P(x)^s e(-nx)\,dx = P^{s-k}\mathfrak{S}(P^\delta, n)J(P^\delta) + O(P^{s-k-\delta'})$$

for some $\delta' > 0$, where

$$\mathfrak{S}(P^\delta, n) = \sum_{q \le P^\delta} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\frac{1}{q}\sum_{m=1}^{q} e(m^k a/q)\right)^s e(-na/q)$$

and

$$J(P^\delta) = \int_{|\gamma|<P^\delta} \left(\int_0^1 e(\gamma\xi^k)\,d\xi\right)^s e(-\gamma)\,d\gamma.$$

Needless to say, this isn't particularly pretty. The so-called "singular series" $\mathfrak{S}(P^\delta, n)$ is rather tricky; it is easy enough to show that we can replace $\mathfrak{S}(P^\delta, n)$ by $\mathfrak{S}(n) := \lim_{X\to\infty} \mathfrak{S}(X, n)$ with acceptable error, but the convergence of this sum is a bit delicate. Fairly elementary arguments suffices to show that it converges as long as $s \ge 2^k + 1$; in fact, in this case it is bounded below (in n) by a constant. We will not discuss this aspect further.

The $J(P^\delta)$ term is easier to deal with. It is easy to show that we can replace it with

$$J = \int_{-\infty}^{\infty} \left(\int_0^1 e(\gamma\xi^k)\,d\xi\right)^s e(-\gamma)\,d\gamma$$

with acceptable error. A fun integration exercise yields

$$J = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)},$$

so in total we have

$$\begin{aligned}\int_M f_P(x)^s e(-nx)\,dx &= \mathfrak{S}(n)P^{s-k}J + O(P^{s-k-\delta'}) \\ &= \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{s/k-1}\mathfrak{S}(n) + O(n^{s/k-1-\delta''}).\end{aligned}$$

Because we expect the integral over the minor arcs to be subsumed into the error terms, this is our expected answer.

7. Minor arcs and conclusion

To estimate the minor arcs, we first do something crude:

$$\left|\int_m f_P(x)^s e(-nx)\,dx\right| \le \int_m |f_P(x)|^s\,dx.$$

Remember, we expect cancellation in f_P itself, so we "don't need the help" that $e(-nx)$ might provide!

This is a classical exponential sum problem, and we have two classical tools that we black-box (neither is terribly difficult, and neither is the best possible):

Theorem 7.1 (Weyl)**.** *Let $f \in \mathbb{R}[X]$ with $\deg f = k$ and highest coefficient α. Also suppose that there exist integers a and q such that $(a,q) = 1$, $q > 0$, and*

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}.$$

Assume that $P^\delta \leq q \leq P^{k-\delta}$ and let $\epsilon > 0$. Then

$$\left|\sum_{i=1}^{P} e(f(i))\right| \ll_{k,\epsilon} P^{1-\delta/2^{k-1}+\epsilon}.$$

That is, we get a tiny bit of improvement over the trivial bound (a factor of $P^{-\delta/2^{k+1}+\epsilon}$ better) so long as α is well-approximated by a fraction with relatively large denominator ($\geq P^\delta$), but not too large ($\leq P^{k-\delta}$).

Theorem 7.2 (Hua)**.** *We have*

$$\int_0^1 |f_P(x)|^{2^k}\, dx \ll_{k,\epsilon} P^{2^k-k+\epsilon}.$$

Again, we get a slight improvement over the trivial bound. Both proofs (of Weyl's inequality and of Hua's) employ induction (on $\deg f$ and k, respectively) and use Cauchy's inequality repeatedly.

Now assume $s \geq 2^k + 1$. On the minor arcs m, we use Dirichlet's theorem on Diophantine approximation to note that x has a rational approximation $\frac{a}{q}$ such that $P^\delta \leq q \leq P^{k-\delta}$ and

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}.$$

Therefore we can apply Weyl's inequality to yield

$$|f_P(x)|^{s-2^k} \ll P^{(s-2^k)(1+\epsilon-\delta/2^{k+1})}.$$

Using Hua's inequality in the third line, we have

$$\begin{aligned}
\int_m |f_P(x)|^s\, dx &= \int_m |f_P(x)|^{s-2^k} |f_P(x)|^{2^k}\, dx \\
&\ll P^{(s-2^k)(1+\epsilon-\delta/2^{k+1})} \int_0^1 |f_P(x)|^{2^k}\, dx \\
&\ll P^{s+\epsilon s-\delta s/2^{k+1}-2^k(1+\epsilon-\delta/2^{k+1})} P^{2^k-k+\epsilon} \\
&\ll P^{s-k-\delta'} \text{ for some } \delta' > 0 \\
&= n^{s/k-1-\delta''}.
\end{aligned}$$

This is indeed something that we can subsume under the error term from the major arcs. Therefore, putting everything together,

$$r_s(n) = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{s/k-1} \mathfrak{S}(n) + O(N^{s/k-1-\delta'})$$

so long as $s \geq 2^k + 1$. Because (as mentioned before) the singular series is bounded below, we get the expected result that $r_s(n) \to \infty$ as $n \to \infty$ whenever $s \geq 2^k + 1$. That is, the number of ways of writing n as a sum of s kth-powers tends to infinity as n does, so long as $s \geq 2^k + 1$.

Heuristically, the quantity

$$\frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{s/k-1}$$

is the "density" of solutions to

$$x_1^k + \ldots + x_s^k = n$$

where the x_i are positive and *real*, while $\mathfrak{S}(n)$ is the term that takes into account congruences between kth powers that make the integers act less regularly than the reals. This can, of course, be made more precise.

8. References

Davenport, H., Analytic methods for Diophantine equations and Diophantine inequalities, Cambridge (2005)

Vaughan, R. C. and Wooley, T. D., *Waring's problem: A survey*, `http://www.math.lsa.umich.edu/~wooley/wps.ps`