The Hardy-Littlewood Circle Method

Sukrith Raman

May 2021

1 Introduction

Is it possible for us to write every number as a sum of two squares? This problem is widely thought about, but has also been solved. We know that a nonnegative integer can be written as a sum of 2 squares if and only if its prime factorization contains no element a^b for $a \equiv 3 \pmod 4$ and b odd. However, is it possible to write every nonnegative integer a a sum of *three* squares? The answer here is also no, as numbers of the form $4^b(8k+7)$ for integers b and k cannot be represented this way. It turns out that every nonnegative integer can be represented as a sum of 4 squares[1]. Another way that we can write this, as we will see later, is $g(2) = 4$, as we need 4 numbers of power 2. How do we see the minimum number of terms with power k needed in order to represent any nonnegative integer? Is there a k for which there is no minimum number of terms, and as n increases, the number of terms needed to represent it does as well? This is known as Waring's problem, who initially conjectured that for all k, $g(k) < \infty$. This was proven to be correct by Hilbert in 1909, but he did not use the Circle Method, as it had not been developed at the time.

2 The Circle Method

First, we can define integers k and s, where k is the exponent of all the terms in the series, and s is the number of terms in the series. As we have mentioned before, $g(k)$ is the function which outputs lowest s for the input k. We can define $\mathbf{x}$ to be the set of numbers $(x_1, x_2, \ldots, x_s)$. Additionally, we can define a function $R(n)$ to be

$$R(n) = R_{s,k}(n) = \{\mathbf{x} \in \mathbf{N}^s : n = \sum_{i=1}^{s} x_i\},$$

or the number of solutions to this sum given the values of s and k. One thing to keep in mind is that all the x_i terms cannot be more than $n^{1/k}$. Hence,

[1] This is known as Lagrange's four square number theorem. You can look it up, but the essence of the proof is that 1. two numbers that can be represented as a sum of four squares can be multiplied to get another number that can be represented this way and 2. every prime can be represented as a sum of four squares.

$1 \leq x_i \leq X$ for $X = \text{floor}(n^{1/k})$[2]. Now, an important integral to introduce is this:

$$\int_0^1 e(\alpha m) d\alpha$$

where $e(\alpha m)$ is just $e^{2\pi i \alpha m}$, but written in a less clunky way. We know that the integral evaluates to 1 if $m = 0$, and is equal to 0 for every other number. From this, it is easy to see that

$$R(n) = \sum_{0 \leq x_1 \leq X} \cdots \sum_{0 \leq x_s \leq X} \int_0^1 e(\alpha(x_1^k + \cdots + x_s^k - n)) d\alpha.$$

This is because we are summing over all the possible values of x_i for each one, and whenever it equals n, the integral evaluates to 1. Summing up 1 n times ultimately gives the value for $R(n)$.

We can now define the function

$$f(\alpha) = f_k(\alpha, X) = \sum_{0 \leq x \leq X} e(\alpha x^k).$$

This lets us rewrite our previous integral/sums as

$$\int_0^1 f(\alpha)^s e(-\alpha n) d\alpha.$$

This may not be obvious at first glance, so we can break it down: the $f(\alpha)^s$ term adds all the x_is together in every possible way that it did in the sums beforehand. If they end up adding to n, then the $e(-\alpha n)$ term cancels that out, leaving the integral to evaluate to 1 n times. The probability that the sum evaluates to n is $O(X^{-k})$, so the expected value of $R(n)$ could be estimated at around $X^s * X^{-k} = X^{s-k}$.

3 Major and Minor arcs

In order to get a better estimate of $R(n)$ using our latest integral form, we need to partition the interval [0, 1] into two different classifications: major and minor arcs. These arcs fulfill the requirement that

$$\int_0^1 f(\alpha)^s e(-\alpha n) d\alpha = \int_M f(\alpha)^s e(-\alpha n) d\alpha + \int_m f(\alpha)^s e(-\alpha n) d\alpha$$

where M represents the parts that are in the major arc and m for the minor one. We can classify the major arc as follows:

$$M = \{x \in \frac{\mathbb{R}}{\mathbb{Z}} : |x - \frac{a}{q}| < X^{\delta - k}\}$$

[2]I don't know how to write the floor function in LaTeX.

for $a \in \mathbb{R}$, $q \in \mathbb{Z}$, and $\delta > 0$, as a very small positive real number. In other words, along this interval, around each fraction $\frac{a}{p}$, there is a small interval which is i the major arc. We ultimately define M as

$$M = \bigcup_{1 \leq a \leq q \leq P^{\delta}} M_{a,q}$$

. These sections hold the most "weight" in the integral, and the minor arc is just everything that the major arc does not take up in the interval.

It turns out that

$$\int_{m} f(\alpha)^s e(-\alpha n) d\alpha = o(X^{s-k})$$

and using something called a singular series $\mathfrak{S}(n)$ and a term J:

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

In total, the major arc becomes

$$\int_{M} f(\alpha)^s e(-\alpha n) d\alpha = \mathfrak{S}(n) P^{s-k} J + o(X^{s-k}).$$

Adding these two arcs together finalizes the integral to be

$$\int_{0}^{1} f(\alpha)^s e(-\alpha n) d\alpha = \mathfrak{S}(n) P^{s-k} J + o(X^{s-k})$$

as $2o(X^{s-k}) = o(X^{s-k})$.

4 Applications

In general, we discussed the function $R(n)$, but this could be generalized as $R(n; s, A)$ with n being the target number, s being the umber of terms we want to combine, and A being the list we choose from. In Waring's Problem, which was discussed so far, A was the set of all perfect integer powers of k, but they can be anything. For example, if A is the set of all primes and s is 3, we get the ternary Goldbach conjecture, which states that all odd numbers 5 or greater can be written as a sum of 3 primes. This statement is equivalent to the better known binary Goldbach conjecture, which states that every even number greater than 5 can be written as a sum of two prime numbers[3].

[3] This can be seen by taking any odd number and subtracting 3, which is prime, to get an even number.