The Circle Method and Class Groups of Quadratic Fields

Carlos Dominguez

Williams College

August 4, 2010

Circle Method

- Want to study sums of d elements from a set A.
  - Waring's problem: sums of s kth powers
  - Goldbach's problem: sums of two or three primes
- Define a generating function for our set:

$$f(x) = \sum_{a \in A} e^{2\pi i a x}$$

- The number of ways n can be represented as the sum of d elements of A is the coefficient of $e^{2\pi i n x}$ in $f(x)^d$, which can be represented by the integral

$$\int_0^1 f(x)^d e^{-2\pi i n x}\, dx$$

- Problem: this integral is hard to calculate.

Major and Minor Arcs

- Observation: f takes on larger-than-average values near rational numbers with small denominators.
- Let $\mathfrak{M}$ (the "major arcs") be the union of small intervals centered at these rational numbers, and $\mathfrak{m}$ (the "minor arcs") be the rest of the unit interval.
- The Circle Method: Estimate the integral on $\mathfrak{M}$ with easier functions that well approximate f on $\mathfrak{M}$, and show that the integral on $\mathfrak{m}$ is small.

A useful theorem (simplified)

Theorem (Perelli, 1996)

If $F \in \mathbb{Z}[x]$ takes on infinitely many even values, then every "short" interval contains "mostly" x such that $F(x)$ is a Goldbach number.

("short" is approximately an interval of width about $N^{1/3}$ around N, "most" is approximately $O(N(\log N)^{-A})$ (A big) potential exceptions.)

An application!

Theorem (Prof. Siman Wong)

For any integer $k > 1$, there exist infinitely many complex quadratic fields for which the Sylow 2-subgroups of their class groups are cyclic of order $\geq 2^k$.

Question: Can we construct quadratic fields with cyclic 2-class groups of exact order 2^k?

Wong shows that if, for any integer $k > 1$, we can find infinitely many pairs of distinct, odd primes p_1, p_2 such that

1. $p_1 + p_2 = 2w^{2^k}$ with w even,
2. $p_1 \equiv 1 \pmod 4$, and
3. $\left(\frac{p_1}{w}\right) = -1$

then $\mathbb{Q}(\sqrt{-p_1 p_2})$ has the desired properties.

This looks like job for...

The Circle Method! (again)

First steps:

- Take $w = 2m^2$. Then $\left(\frac{p_1}{w}\right) = -1 \implies \left(\frac{p_1}{2}\right) = -1 \implies p_1 \equiv \pm 3 \bmod 8$.
- Cue to study how the circle method works with sets of primes in particular congruence classes.

12 pages of mess later...

- It works (believe me). In particular:

Theorem (SMALL 2010)

If $F \in \mathbb{Z}[x]$ takes on infinitely many even values not congruent to 4 mod 8, *then there are infinitely many x such than $F(x)$ can be written as the sum of two primes congruent to* 3 *and* 5 mod 8.

Taking $F(x) = 2(2x^2)^{2^k}$ gives therefore gives us the desired result. That is...

One last theorem

Theorem (SMALL 2010)

Given any integer $k > 1$, there exist infinitely many complex quadratic fields with cyclic 2-class group of order exactly 2^k.