The Circle Method and Class Groups of Quadratic Fields

Carlos Dominguez

Ohio State University

August 28, 2010

Definitions

Definition

A **number field** is a finite extension of the field of rationals. For example: $\mathbb{Q}(i)$, the Guassian rationals, or $\mathbb{Q}(\sqrt{d})$, the quadratic fields for squarefree d.

Definition

An **algebraic integer** is any root of a monic polynomial with integer coefficients. The set of all algebraic integers in a number field forms a ring, called the **ring of integers** in a number field.

Definitions (cont'd.)

Definition

Let K be a number field. Define an equivalence relation $\sim$ on the fractional ideals of K by $I \sim J$ if there exist non-zero $\alpha, \beta \in K$ such that $\alpha I = \beta J$. The group formed by these equivalence classes of fractional ideals (under the obvious multiplication: $[IJ] = [I][J]$) is called the **class group** of K.

Definition

If the class group is finite, then the order of the class group is called the **class number**.

Why should we care?

The structure of the class group has intimate connections with many areas of algebra and number theory including, but not limited to:

- Describing how badly a ring of integers in a number field fails to have unique factorization

Why should we care?

The structure of the class group has intimate connections with many areas of algebra and number theory including, but not limited to:

- Describing how badly a ring of integers in a number field fails to have unique factorization
- Class field theory and Galois theory

Why should we care?

The structure of the class group has intimate connections with many areas of algebra and number theory including, but not limited to:

- Describing how badly a ring of integers in a number field fails to have unique factorization
- Class field theory and Galois theory
- Dirichlet's class number formula and primes in arithmetic progressions

Why should we care?

The structure of the class group has intimate connections with many areas of algebra and number theory including, but not limited to:

- Describing how badly a ring of integers in a number field fails to have unique factorization
- Class field theory and Galois theory
- Dirichlet's class number formula and primes in arithmetic progressions
- Professor says I should care/pays my salary.

Cyclicity of the 2-class group

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 $\geq 2^k$.

Cyclicity of the 2-class group

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?

Cyclicity of the 2-class group

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,

Cyclicity of the 2-class group

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. $p_1 \equiv 1 \pmod 4$

Cyclicity of the 2-class group

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.

An initial stab...

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 sums of pairs of primes in particular congruence classes.
- Specifically, what can we prove about representing values of a polynomial as the sum of two primes congruent to 3 and 5 mod 8?

A useful theorem (simplified)

Theorem (Perelli, 1996)

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

("short" is approximately an interval of width about $N^{1/3}$ around N)

Corollary (What we basically care about is...)

Infinitely many values of F can be written as the sum of two primes.

The Circle Method

- Want to study sums of d elements from a set A.

The Circle Method

- Want to study sums of d elements from a set A.
  - Waring's problem: sums of s kth powers

The 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

The 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 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

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

The 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.

The Basics: Major and Minor Arcs

- Observation: f takes on larger-than-average values near rational numbers with small denominators.

The Basics: 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 Basics: 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.

The Basics: 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.
- Typically we only care about showing existence of at least one representation; that is,

$$\int_{\mathfrak{M}} f(x)^d e^{-2\pi inx}\,dx + \int_{\mathfrak{m}} f(x)^d e^{-2\pi inx}\,dx \geq 1$$

. Hence sloppy estimation ~~acceptable~~ encouraged!

The Prime Case: Major Arcs

Define the weighted prime generating function

$$f(\alpha) = \sum_{p \leq n} (\log p) e^{2\pi i p \alpha}$$

Lemma

Let

$$v(\beta) = \sum_{m=1}^{n} e^{2\pi i \beta m}.$$

Then there is a positive constant C such that, for all α in a major arc around a/q ($(a, q) = 1$),

$$f(\alpha) = \frac{\mu(q)}{\phi(q)} v(\alpha - a/q) + O(n \exp(-C(\log n)^{1/2})).$$

Things get nicer . . .

Now to study sums of two primes, we want to look at coefficients of $f(\alpha)^2$. But we now have that

$$f(\alpha)^2 - \frac{\mu(q)^2}{\phi(q)^2} v(\alpha - a/q)^2 \ll n^2 \exp(-C(\log n)^{1/2})$$

Estimating integrals with $f(\alpha)^2$ is now much easier:

- v is a much easier function to study.
    - does not depend on prime sums. Primes are hard.
    - Exponentials: easy to integrate.
- μ and ϕ are easily bounded

The Singular Series

- (The minor arc calculation is a rather tedious application of Weyl's inequality; we'll skip it for brevity.)
- Summing and integrating our estimates naturally gives rise to the so-called "singular series":

$$\mathfrak{S}(m) = \left(\prod_{p \nmid m} (1 - (p-1)^{-2})\right) \left(\prod_{p \mid m} (1 + (p-1)^{-1})\right)$$

Theorem

$$\sum_{m=1}^{n} |R(m) - m\mathfrak{S}(m)|^2 \ll n^3 (\log n)^{-A}$$

where $R(m)$ is the coefficient of $e^{2\pi i m\alpha}$ in $f(\alpha)^2$ – that is, the number of ways of writing m as the sum of two primes – and A is a large integer.

Some functions

Definition

We restrict f by the function

$$f_2(\alpha) = \sum_{p \leq n} (\log p) e^{2\pi i p \alpha},$$

where the primes are restricted to those congruent to those congruent to 3 or 5 mod 8.

Some functions

Definition

We restrict f by the function

$$f_2(\alpha) = \sum_{p \le n} (\log p) e^{2\pi i p \alpha},$$

where the primes are restricted to those congruent to those congruent to 3 or 5 mod 8.

Definition

To estimate f_2, we define a function μ_2 by

- $\mu_2(q) = \mu(q)/2$ whenever $8 \nmid q$
- $\mu_2(8) = -\sqrt{2}$, and
- $\mu_2(8q) = \left(\frac{q}{2}\right)|\mu(q)|\sqrt{2}$ for $q > 1$.

Generalization Results

Lemma (D– 2010)

$$f_2(\alpha)^2 - \frac{\mu_2(q)^2}{\phi(q)^2} v(\alpha - a/q)^2 \ll n^2 \exp(-C(\log n)^{1/2}),$$

where α is in the major arc around a/q.

Generalization Results

Lemma (D– 2010)

$$f_2(\alpha)^2 - \frac{\mu_2(q)^2}{\phi(q)^2} v(\alpha - a/q)^2 \ll n^2 \exp(-C(\log n)^{1/2}),$$

where α is in the major arc around a/q.

Theorem (D– 2010)

$$\sum_{m=1}^{n} |R(m) - m\mathfrak{S}_2(m)|^2 \ll n^3 (\log n)^{-A}$$

where $R_2(m)$ is the coefficient of $e^{2\pi i m\alpha}$ in $f_2(\alpha)^2$, and $\mathfrak{S}_2$ is a similar series to $\mathfrak{S}_2$, usually equal to $\mathfrak{S}/4$ or $\mathfrak{S}/2$.

Theorem (D– 2010)

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

Back on the algebraic side of things, we can take $F(x) = 2(2x^2)^{2^k}$ in the above theorem to finally prove:

Theorem (D– 2010)

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