An application of Vinogradov's method to class groups

Peter Koymans
Universiteit Leiden

Soest 2016

Diamant symposium

Soest, The Netherlands, November 2016

Class groups

Let K be a number field and let $\mathcal{O}_K$ and Cl_K denote its ring of integers and its class group respectively.

The finite abelian group Cl_K encodes useful information about the arithmetic in $\mathcal{O}_K$.

The class group of a number field is therefore one of the most fundamental and well-studied invariants in number theory.

In the case of quadratic number fields, the most accessible part of the class group is its 2-part.

The 2-part of $Cl_{\mathbb{Q}(\sqrt{-p})}$

We look at a very special family of number fields $\mathbb{Q}(\sqrt{-p})$, where p is a prime number. Let $Cl_{\mathbb{Q}(\sqrt{-p})}$ be its class group. We are interested in the 2-part of $Cl_{\mathbb{Q}(\sqrt{-p})}$, i.e.

$$Cl_{\mathbb{Q}(\sqrt{-p})}[2^\infty] := \{g \in Cl_{\mathbb{Q}(\sqrt{-p})} : \text{the order of } g \text{ is a power of } 2\}.$$

Theorem 1 (Gauss's genus theory)

The group $Cl_{\mathbb{Q}(\sqrt{-p})}[2^\infty]$ is cyclic, so $Cl_{\mathbb{Q}(\sqrt{-p})}[2^\infty] \cong \mathbb{Z}/2^n\mathbb{Z}$ for some integer $n \geq 0$.

Definition 2

Write $h_p := |Cl_{\mathbb{Q}(\sqrt{-p})}[2^\infty]|$. By Theorem 1 h_p determines the isomorphism class of $Cl_{\mathbb{Q}(\sqrt{-p})}[2^\infty]$.

Previous results

The following results are known:

$$2 \mid h_p \Leftrightarrow p \equiv 1 \mod 4$$
$$4 \mid h_p \Leftrightarrow p \equiv 1 \mod 8$$
$$8 \mid h_p \Leftrightarrow p \equiv 1 \mod 8 \text{ and } \left(\frac{1+i}{p}\right) = 1.$$

Each of the conditions on the right hand side is equivalent to p splitting completely in some number field K. Then density results follow immediately from Chebotarev's Density Theorem.

Can we continue this?

In view of the previous results one can hope to find a number field K such that $16 \mid h_p$ if and only if p splits completely in K. However, such a field has not been found yet.
Despite this obstacle we prove that the primes p for which $16 \mid h_p$ has the density as predicted by the Cohen-Lenstra heuristics, namely $\frac{1}{16}$.

Theorem 3 (joint with Djordjo Milovic)

Let p be a prime number such that $8 \mid h_p$. Let $e_p = 1$ if $Cl_{\mathbb{Q}(\sqrt{-p})}$ if $16 \mid h_p$ and $e_p = -1$ otherwise. Then there exists an absolute constant $\delta > 0$ such that

$$\sum_{\substack{p \leq X \\ 8 \mid h_p}} e_p \ll X^{1-\delta}$$

under the assumption of a short character sum conjecture.

Vinogradov's method

Let $\{a_p\}$ be a sequence of complex numbers of absolute value bounded by 1 indexed by the prime numbers. Suppose that one wishes to show a "power-saving" estimate for $\{a_p\}$, i.e.

$$\sum_{p \leq X} a_p \ll X^{1-\delta} \text{ for some absolute constant } \delta > 0. \tag{1}$$

Vinogradov's method

Suppose we can extend $\{a_p\}$ to a sequence $\{a_n\}_{n \in \mathbb{Z}_{>0}}$, also of absolute value bounded by 1, for which we can prove power-saving estimates for

$$\sum_{\substack{n \leq N \\ n \equiv 0 \mod d}} a_n,$$

which are called congruence sums, and for

$$\sum_{m \leq M} \sum_{n \leq N} \alpha_m \beta_n a_{mn},$$

which are called general bilinear sums, then (1) holds.

The proof

Suppose that $8 \mid h_p$. We need a criterion of the shape

$$16 \mid h_p \Leftrightarrow f(p) = 1,$$

where $f(p) \in \{\pm 1\}$. Several such criteria are known, but we use a criterion due to Bruin and Hemenway. After some reduction steps $f(p)$ becomes similar to a so-called "spin symbol".

A "spin symbol" is a Jacobi symbol of the shape

$$\left(\frac{\sigma(\alpha)}{\alpha}\right)_K,$$

where K is a fixed number field and σ is a fixed automorphism of K.

Such a "spin symbol" has been dealt with in a paper due to Friedlander, Iwaniec, Mazur and Rubin using Vinogradov's method. We managed to adapt their proof to our setting.

The proof II

Our estimate for the bilinear sums is standard and follows the earlier mentioned paper by Friedlander, Iwaniec, Mazur and Rubin. For the congruence sums we needed a novel idea, based on lattice point counting and the geometry of numbers. We sketch the new idea here.

Let K be a number field of degree n, $\mathcal{O}_K$ its ring of integers and $\mathbb{M}$ a submodule of $\mathcal{O}_K$ of rank r "sufficiently large".

Definition 4

Let $\alpha \in \mathcal{O}_K$ and factor $(\alpha) = \mathfrak{g}\mathfrak{q}$, where $N\mathfrak{g}$ and $N\mathfrak{q}$ are co-prime, $N\mathfrak{g}$ is square-full and $N\mathfrak{q}$ is square-free. Then we call $\mathfrak{g}$ the square-full part of α.

Goal: estimate the number of $\alpha \in \mathbb{M}$ with $|\alpha^{(i)}| \leq X^{1/n}$ such that the square-full part of α is large, i.e. $N\mathfrak{g} \geq X^{\delta}$ for some fixed $\delta > 0$.

The solution

Fix $\mathfrak{g}$ for now and a basis of $\mathbb{M}$, so we can identify $\mathbb{M}$ with $\mathbb{Z}^r$. We are going to estimate

$$E_{\mathfrak{g}}(X) := \{\alpha \in \mathbb{M} : \alpha \equiv 0 \mod \mathfrak{g}, |\alpha^{(k)}| \leq X^{1/n} \text{ for all } k\}$$

instead. Define

$$\Lambda_{\mathfrak{g}} := \{\alpha \in \mathbb{M} : \alpha \equiv 0 \mod \mathfrak{g}\}$$

and

$$S_X := \{(a_1, \ldots, a_r) \in \mathbb{R}^r : a_i \ll X^{1/n}\}.$$

Then $|E_{\mathfrak{g}}(X)| \leq |\Lambda_{\mathfrak{g}} \cap S_X|$.

The solution II

Now apply lattice point counting techniques. These imply that

$$|\Lambda_{\mathfrak{g}} \cap S_X| \approx \left| \frac{\mathrm{Vol}(S_X)}{\det \Lambda_{\mathfrak{g}}} \right|$$

up to some error depending on the successive minima of the lattice $\Lambda_{\mathfrak{g}}$.

Key observation: the first successive minimum, i.e. the length of the shortest non-zero vector of $\Lambda_{\mathfrak{g}}$, is large. In combination with Minkowski's theorem on successive minima of symmetric convex bodies this allows us to control the error term and also $\det \Lambda_{\mathfrak{g}}$.