$2^k$-class groups of imaginary quadratic fields

Alexander Smith

19 January 2019
Cohen-Lenstra heuristics for imaginary quadratic fields

Given a number field $K$, $\text{Cl} K$ will denote its class group. For any positive integer $n$, $\text{Cl} K[n]$ will denote the $n$-torsion of this group.

**Conjecture (Cohen-Lenstra 1983)**

Take $p$ to be an odd prime, and take $H$ to be a finite abelian $p$-group. Then

$$\lim_{N \to \infty} \frac{\# \{ 0 < d < N : \text{Cl} \mathbb{Q}(\sqrt{-d})[p^\infty] \cong H \}}{N} \propto \frac{1}{|\text{Aut} H|}.$$  

This conjecture made no prediction for what happens for $p = 2$. 
Choose a sequence \( p_1, \ldots, p_r \) of distinct primes, and take \( d \) to be their product. For simplicity, assume that \( d \) equals 3 mod 4.

As an \( \mathbb{F}_2 \) vector space, \( \text{Cl} \mathbb{Q}(\sqrt{-d})[2] \) is \( r - 1 \) dimensional, with a basis of ideals

\[
(p_1, \sqrt{-d}), \quad (p_2, \sqrt{-d}), \quad \ldots, \quad (p_{r-1}, \sqrt{-d}).
\]

Most positive integers less than \( N \) have about \( \log \log N \) prime factors.

So the 2-torsion of class groups tends to grow without bound for imaginary quadratic fields.
Cohen-Lenstra-Gerth heuristics

Conjecture (Gerth 1987)

Take \( p \) to be a prime, and take \( H \) to be a finite abelian \( p \)-group. Then

\[
\lim_{N \to \infty} \frac{\# \{ 0 < d < N : 2\text{Cl} \mathbb{Q}(\sqrt{-d})[p^\infty] \cong H \}}{N} \propto \frac{1}{|\text{Aut} \ H|}.
\]

Three theorems have been proved towards this conjecture:

- (Davenport-Heilbronn 1971) The average size of \( \text{Cl} \mathbb{Q}(\sqrt{-d})[3] \) is 2.
- (Fouvry-Klüners 2006) The groups \( 2\text{Cl} \mathbb{Q}(\sqrt{-d})[4] \) have a distribution consistent with the conjecture.
- (S. 2017) The conjecture is correct for \( p = 2 \).
Class groups as cokernels

Theorem (Friedman-Washington 1989)

Take \( p \) to be a prime, and take \( H \) to be a finite abelian \( p \)-group. Take \( M_n \) to be a random \( n \times n \) matrix with entries uniformly and independently chosen from \( \mathbb{Z}_p \). Then

\[
\lim_{n \to \infty} \mathbb{P}(\text{coker } M_n \cong H) \propto \frac{1}{|\text{Aut } H|}.
\]

Given \( n \geq j \geq 0 \), take \( P^{\text{Mat}}(j|n) \) to be the probability a uniformly selected \( n \times n \) matrix with entries in \( \mathbb{F}_2 \) has kernel of dimension \( j \).
Main result

Define the $2^k$-class rank of $\mathbb{Q}(\sqrt{-d})$ to be the maximal $r$ for which there is an injection from $(\mathbb{Z}/2^k\mathbb{Z})^r$ to $\text{Cl} \mathbb{Q}(\sqrt{-d})$. Write $r_k(d)$ for the $2^k$-class rank of $\mathbb{Q}(\sqrt{-d})$.

**Theorem (S. 2017)**

For $k > 2$ and $r_2 \geq r_3 \geq \cdots \geq r_k \geq 0$,

$$\lim_{N \to \infty} \frac{\# \{ 0 < d < N : r_i(d) = r_i \text{ for } i \leq k \}}{\# \{ 0 < d < N : r_i(d) = r_i \text{ for } i \leq k - 1 \}} = P^{\text{Mat}}(r_k \mid r_{k-1}).$$

**Theorem (Fouvry-Klüners 2006)**

For $r_2 \geq 0$,

$$\lim_{N \to \infty} \frac{\# \{ 0 < d < N : r_2(d) = r_2 \}}{N} = \lim_{n \to \infty} P^{\text{Mat}}(r_2 \mid n).$$
Class ranks as a Markov chain

Class rank transition probabilities

Table: Probability the $2^k$-class rank is $r$.

<table>
<thead>
<tr>
<th></th>
<th>$r$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>4-class</td>
<td>.29</td>
</tr>
<tr>
<td>8-class</td>
<td>.63</td>
</tr>
<tr>
<td>16-class</td>
<td>.81</td>
</tr>
<tr>
<td>32-class</td>
<td>.91</td>
</tr>
<tr>
<td>64-class</td>
<td>.95</td>
</tr>
<tr>
<td>$2^\infty$-class</td>
<td>1</td>
</tr>
</tbody>
</table>
Results for Selmer groups

For $E : y^2 = x^3 + ax + b$ an elliptic curve over $\mathbb{Q}$, and for $d$ a positive integer, define a twisted curve

$$E^d : y^2 = x^3 + d^2 ax + d^3 b.$$ 

For $k \geq 1$, the $2^k$-Selmer groups of these objects are analogous to the $2^{k+1}$-class groups of quadratic fields.

If $E$ satisfies certain technical conditions, we proved that the $2^k$-Selmer ranks of its twists are described by an analogous Markov chain.
Results for Selmer groups

Theorem (S. 2019)

Suppose $E/\mathbb{Q}$ obeys the above conditions. Among the twists $E^d$,

- $50\%$ have $2^\infty$-Selmer corank 0,
- $50\%$ have $2^\infty$-Selmer corank 1, and
- $0\%$ have higher $2^\infty$-Selmer corank.

Assuming $\text{III}(E^d)$ is finite, the $2^\infty$-Selmer corank of $E^d$ equals its actual rank.

Under this hypothesis, the above theorem confirms Goldfeld’s conjecture for $E$. 
Controlling 4-class ranks

Choose a sequence \( p_1, \ldots, p_r \) of distinct primes, and write \( d \) for their product. Assume \( d \) equals 3 mod 4.

Given a positive integer \( b \) dividing \( d \), we have

\[
(b, \sqrt{-d}) \in 2\text{Cl} \mathbb{Q}(\sqrt{-d})[4]
\]

iff there is a nonzero ideal \( I \) of \( \mathbb{Q}(\sqrt{-d}) \) and integers \( x, y \) so that

\[
(b, \sqrt{-d}) I^2 = (x + y\sqrt{-d}).
\]

This holds iff there are integers \( x, y, z \) with \( z \) nonzero so that

\[
.bz^2 = x^2 + dy^2.
\]

This is solvable over \( \mathbb{Z} \) if it is solvable in \( \mathbb{Q}_{p_i} \) for each \( i \leq r \).

The 4-class rank can be calculated from the Legendre symbols

\[
\left( \frac{p_i}{p_j} \right), \quad i, j \leq r, \quad i \neq j.
\]
Theorem

Take \( b \) to be a positive integer, and take

\[
K_b = \mathbb{Q} \left( \sqrt{c} : c \in \mathbb{Z}, c \mid 2b \right).
\]

Then, for \( p \) not dividing \( 2b \), we can calculate the 4-class rank of \( \mathbb{Q}(\sqrt{-bp}) \) from the value of

\[
\text{Frob } p \quad \text{in} \quad \text{Gal}(K_b/\mathbb{Q}).
\]

The distribution of 4-class ranks can be derived as a consequence of the Chebotarev density theorem and the Bombieri-Vinogradov theorem.
Theorem (Rédei and others)

*Given a positive integer $b$, there is a finite elementary 2-abelian extension*

$$M_b/K_b \text{ Galois above } \mathbb{Q}$$

*so that, for any $p$ not dividing $2b$, we can determine the 8-class rank of $\mathbb{Q}(\sqrt{-bp})$ from the conjugacy class of*

$$\text{Frob}_p \text{ in } \text{Gal}(M_b/\mathbb{Q}).$$

*This means there is a function $\phi_b$ from $\text{Gal}(M_b/\mathbb{Q})$ to the integers so that the 8-class rank of $\mathbb{Q}(\sqrt{-bp})$ is $\phi_b(\text{Frob}_p)$.*
Split the positive integers into rectangles with $b$ on one axis, $p$ the other.

For most $b$, the 8-rank $\phi_b(\sigma)$ has the distribution we expect as $\sigma$ varies over $\text{Gal}(M_b/\mathbb{Q})$.

Chebotarev
Governing fields for 16-class ranks

They probably don’t exist.
Partial governing fields

Fix $k > 2$.

- We can find tuples $b = (b_1, \ldots, b_m)$ of positive integers so there is a finite Galois extension $M_b/\mathbb{Q}$ and a class function

$$
\Phi : \text{Gal}(M_b/\mathbb{Q}) \longrightarrow \text{Collections of } m\text{-tuples of finite abelian 2-groups}
$$

so that, for $p$ not dividing $2b_1 \ldots b_m$, $\Phi(\text{Frob } p)$ contains

$$
\left( \text{Cl } \mathbb{Q}(\sqrt{-b_1 p})[2^k], \ldots, \text{Cl } \mathbb{Q}(\sqrt{-b_m p})[2^k] \right)
$$

- If $m$ is large, and if $\sigma$ is chosen in $\text{Gal}(M_b/\mathbb{Q})$ to avoid a certain low-density bad subset, then every tuple of groups in $\Phi(\text{Frob } p)$ has approximately the distribution we expect.
Governing fields vs. partial governing fields

Non-generic $M_{b}/\mathbb{Q}$

Chebotarev is used to enforce equidistribution
Governing fields vs. partial governing fields

Chebotarev is used to enforce equidistribution

Chebotarev is used to avoid bad Frob $p$