Unconditional computation of the class groups of real quadratic fields

Andrei Seymour-Howell
Joint work with Ce Bian, Andrew Booker, Austin Docherty and Michael Jacobson Jr.

University of Bristol

CIRM - Building Bridges 6 - 12th September 2024

Uses of computing class numbers for automorphic forms

Imaginary class numbers are used to compute holomorphic modular forms using a trace formula.

Real quadratic class numbers are used to compute Maass forms, again using a trace formula.

More class numbers = More automorphic forms

Numerical verification of the Selberg eigenvalue conjecture up to level 880 by Booker, Lee and Strömbergsson also uses real quadratic class numbers.

Previous computations of real quadratic fields

Source	Bound	Invariants
Gauss	$\Delta < 1000$	h_Δ
Saito and Wada 1988	$\Delta < 10^6$	Cl_Δ, R_Δ
Jacobson 1998	$\Delta < 10^9$	Cl_Δ, R_Δ
te Riele and Williams 2003	$p < 2 \cdot 10^{11}$, $p \equiv 1 \pmod 4$	h_Δ, R_Δ

Hafner and McCurley: $O(\exp((\log \Delta)^{1/2+\varepsilon}))$ (runtime heuristic)

Buchmann: $O(\Delta^{1/4+\varepsilon})$

Lenstra/Shanks: $O(\Delta^{1/5+\varepsilon})$

Unfortunately, these algorithms all rely on GRH.

Imaginary quadratic fields

For the case of imaginary quadratic fields Ramachandran, Jacobson, and Williams used modular forms to unconditionally compute and verify class numbers of imaginary quadratic fields.

Idea:

1) Compute a list of class numbers for imaginary quadratic fields up to discriminant of size say X. With Buchmann's algorithm, you would get a lower bound to the size of the class numbers.

2) Use the trace formula for holomorphic forms of fixed weight and level to derive an upper bound and compare the two.

In fact, in their algorithm no modular forms are needed, since we can choose a space of fixed weight and level that is empty and still derive a non-trivial expression for the class numbers.

Maass cusp forms

We call a function $f : \mathbb{H} \to \mathbb{C}$ a **Maass cusp form** on $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ if

1) f is automorphic, $f(\gamma z) = f(z)$ for all $\gamma \in \Gamma$,
2) f is an eigenfunction of the Laplacian, $\Delta f = \lambda f, \lambda \geq 0$,
3) $f \in L^2(\Gamma\backslash\mathbb{H})$, i.e f is square-integrable,
4) f vanishes at the cusp of $\Gamma\backslash\mathbb{H}$.

For any f and any non-zero integer n, we have the **Hecke operator** T_n that maps Maass forms to Maass forms. Further f has a Fourier expansion of the form

$$f(z) = f(x + iy) = \sum_{n \neq 0} a(n)\sqrt{y} K_{ir}(2\pi|n|y) \exp(2\pi i n x)$$

where $K_\nu(u)$ is the K-Bessel function and $\lambda = \frac{1}{4} + r^2$.

Selberg trace formula

The Selberg trace formula allows one to consider the whole spectrum of Maass cusp forms. Selberg derived this in the 1950's to prove the existence of Maass cusp forms.

In our case, if we have a Hecke eigenbasis $\{f_j\}$ of level 1 Maass cusp forms with respective Laplace eigenvalues $\lambda_j = \frac{1}{4} + r_j^2$ and Hecke eigenvalues $a_j(n)$, the Selberg trace formula allows us to compare

$$\text{(Spectral side)} \sum_{j=1}^{\infty} a_j(n) H(\lambda_j) = \text{(Geometric side)}$$

for some nice (analytic) test function H and $n \neq 0$.

Explicit trace formula

Important for us, is that the geometric side contains class numbers of real quadratic fields! Explicitly, let g be the Fourier transform of h, then

$$\sum_{j=1}^{\infty} a_j(n)h(r_j) = \sum_{\substack{t\in\mathbb{Z} \\ \sqrt{D}=\sqrt{t^2-4n}\notin\mathbb{Q} \\ D>0}} L(1,\psi_D)g\left(\log\left(\frac{(|t|+\sqrt{D})^2}{4n}\right)\right) + \Psi(n),$$

where, with $D = d\ell^2$, we have

$$L(1,\psi_D) = \frac{L(1,\psi_d)}{\ell}\prod_{p|\ell}\left[1+(1-\psi_d(p))\frac{(\ell,p^\infty)-1}{p-1}\right].$$

Idea of the algorithm

Choosing a specific test function, we can write the trace formula as

$$\sum_{j=1}^{\infty} a_j(n)h(r_j) = \sum_{\substack{t\in\mathbb{Z} \\ \sqrt{D}=\sqrt{t^2-4n}\notin\mathbb{Q} \\ 0<D\leq X}} L(1,\psi_D)\left(1-\frac{D}{X}\right)^k + \Psi(n).$$

Truncating the spectral sum and rearranging, we have

$$\sum_{\substack{t\in\mathbb{Z} \\ \sqrt{D}=\sqrt{t^2-4n}\notin\mathbb{Q} \\ 0<D\leq X}} L(1,\psi_D)\left(1-\frac{D}{X}\right)^k = \sum_{r_j\leq R} a_j(n)h(r_j) + E_n - \Psi(n).$$

Idea of the algorithm

1) Compute the class number and regulator for real quadratic fields up to discriminant X (plus a little extra). Recall Buchmann's will give a lower bound to the size of the class number unconditionally.

2) Also compute the spectral side of the trace formula for all $n \leq \sqrt{X}$ and a bound for the error E_n. This will be used as a upper bound on the size of the class numbers.

3) To verify a given class number, we double it in the hyperbolic sum. If this breaks RHS of the above equation we get a contradiction and thus our class number was correct.

For part 2), we need to rigorously compute the Laplace eigenvalues and all Hecke eigenvalues up to $\sqrt{X}$ for several Maass cusp forms.

Complexity

Buchmann's algorithm computes the class number in $O(\Delta^{1/4+\varepsilon})$. Due to work of De Haan, Jacobson and Williams, we can unconditionally compute the regulator in $O(\Delta^{1/6+\varepsilon})$. Thus to compute all class numbers and regulators up to discriminant X is $O(X^{5/4+\varepsilon})$.

We need to compute the trace formula for all $n \leq \sqrt{X}$. This computation is dominated by computing the hyperbolic terms, of which there are roughly X. Hence the verification can be done in $O(X^{1+\varepsilon})$.

Overall, we get $O(X^{5/4+\varepsilon})$ to compute and unconditionally verify all class numbers up to discriminant X.

Implementation

We implemented this algorithm and have unconditionally computed all class numbers and regulators up to discriminant $X = 10^{11}$.

To do this, we computed the Laplace eigenvalues of the first 2184 Maass forms of level 1, and all Hecke eigenvalues a_n with $n \leq \sqrt{X}$.

We are currently running this code to improve this bound to $X = 2^{40} \approx 10^{12}$.

Can we do better?

For the imaginary quadratic field case, to compute the class number Jacobson and Mosunov used a relation between the Fourier coefficients of one of the classical Jacobi theta function and the Hurwitz class number. Computing the Fourier coefficients can be done in subexpontential time.

Something similar should be possible for real quadratic fields. Goldfeld and Hoffstein (1985) derived a half-integral weight Eisenstein series whose Fourier coefficients are related to $L(1, \chi_\Delta)$ for $\Delta > 0$.

Using Hejhal's algorithm one could compute the Fourier coefficients, and hence the $L(1, \chi_\Delta)$ value in subexponential time. However, to get the class number we would still need the regulator. Hence currently unconditionally, the best speed we could obtain is $O(X^{7/6+\varepsilon})$ to compute all class numbers up to discriminant X.

Cohen–Lenstra heuristics

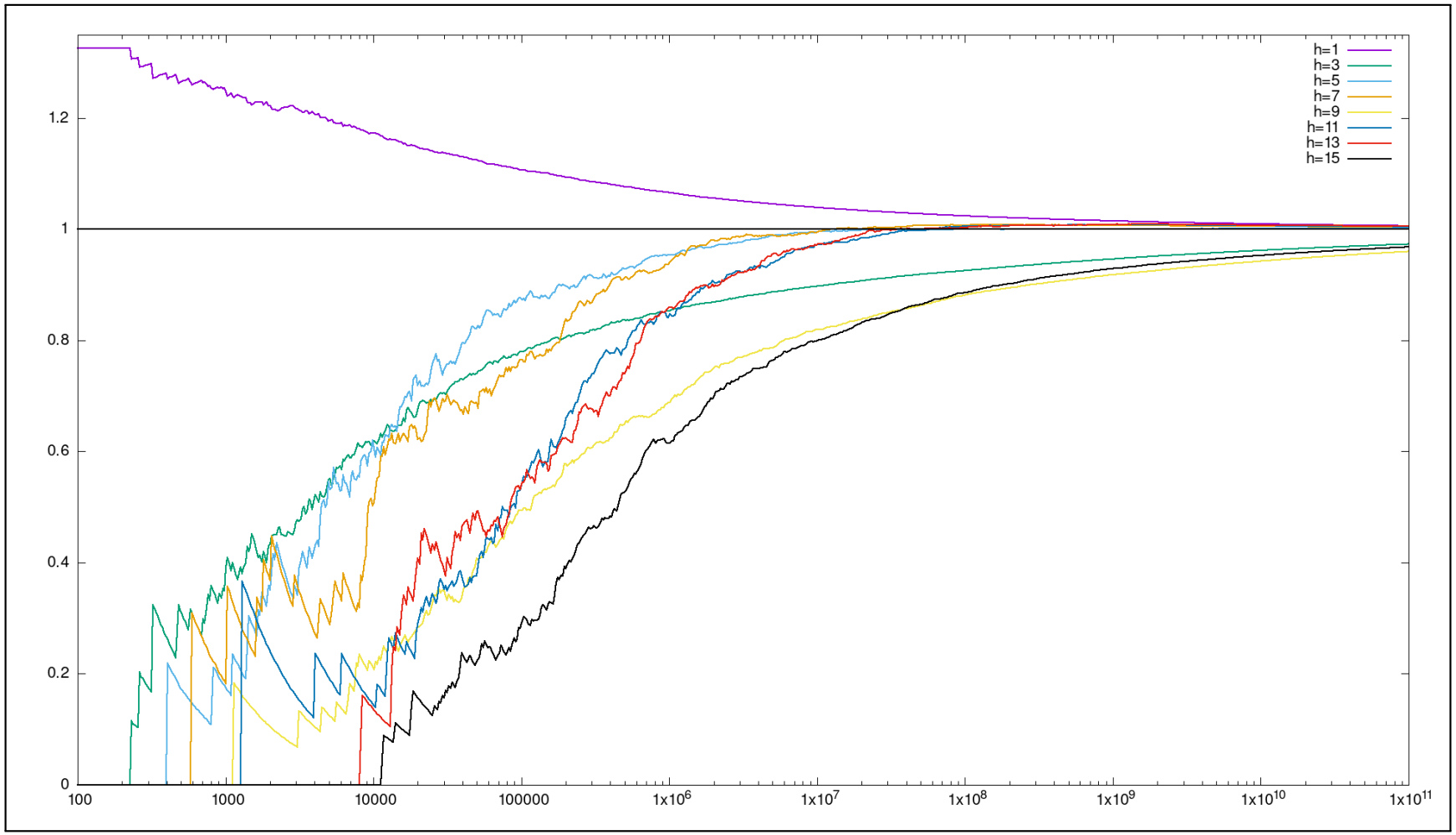

Figure: Ratio of actual and expected frequencies of odd class number h over $\Delta \leq X$.

Cohen–Lenstra heuristics

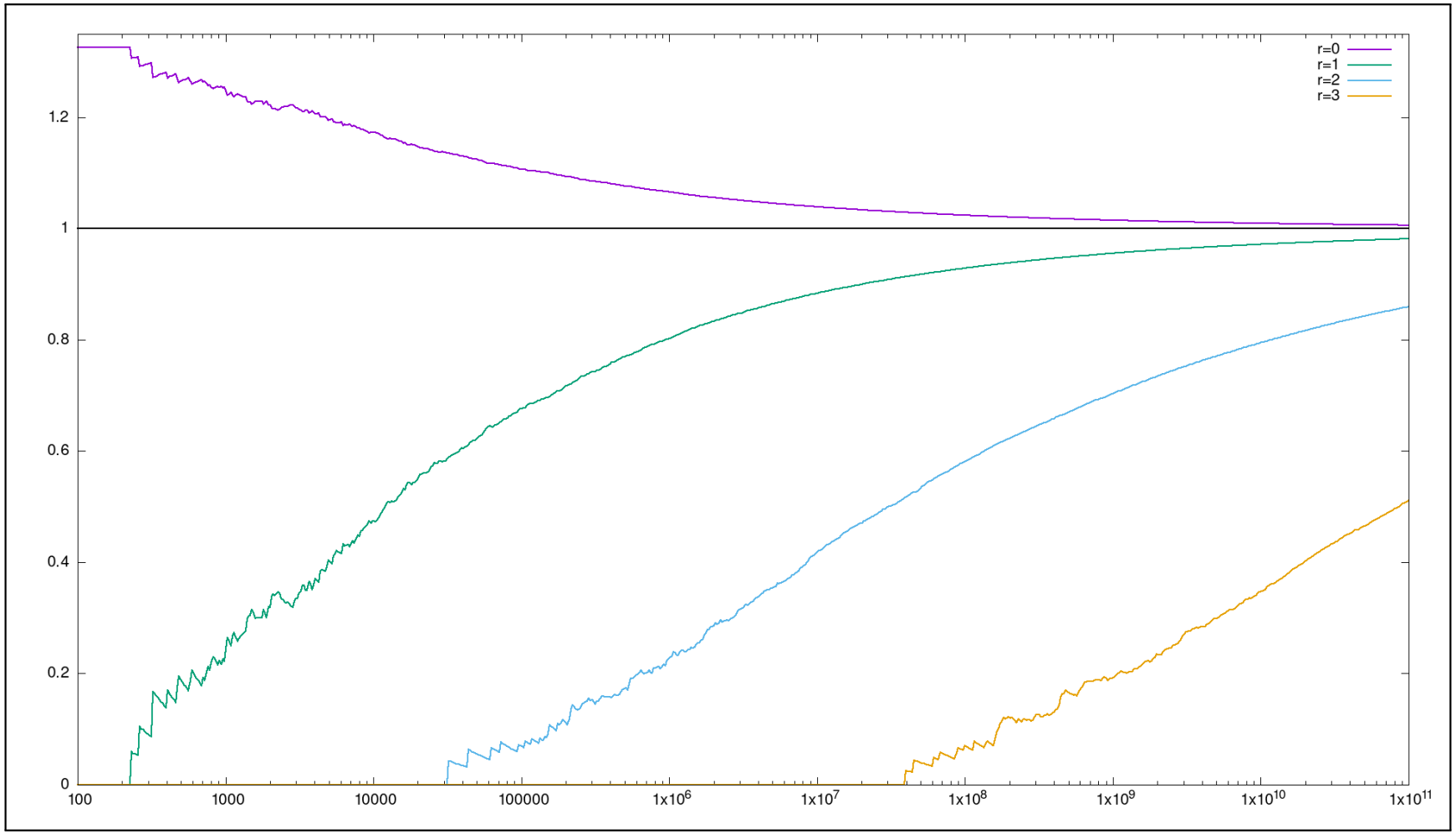

Figure: Ratio of actual and expected frequencies of odd rank r over $\Delta \leq X$.

Thanks for listening!