Tabulating Class Groups of Imaginary Quadratic Fields

Michael J. Jacobson, Jr.

UNIVERSITY OF CALGARY

Joint work with A. Mosunov

WCNT, December 16, 2015

Tabulating Class Groups

Let:

- $\mathbb{Q}(\sqrt{\Delta})$ be the imaginary quadratic field of negative (fundamental) discriminant $\Delta \equiv 0, 1 \pmod 4$
- Cl_Δ be the ideal class group of the maximal order $\mathcal{O}_\Delta$
- $h_\Delta = |Cl_\Delta|$ the class number

Goal: for all $\mathbb{Q}(\sqrt{\Delta})$ with $|\Delta| \leq M$ as large as possible compute

- h_Δ
- structure of $Cl_\Delta \cong C(m_1) \times C(m_2) \times \cdots \times C(m_r)$, where $m_{i+1} \mid m_i$

Want *unconditional* results as numerical evidence supporting conjectures (e.g. Cohen-Lenstra). No Riemann Hypotheses allowed!

Previous Tabulations (Highlights)

Gauß (1801): tables of all Δ with given small h_Δ

Buell (1999): $|\Delta| < 2.2 \times 10^9$

- counting reduced positive definite binary quadratic forms

Ramachandran, J., Williams (2006): $|\Delta| < 2 \times 10^{11}$:

- compute class groups using generic algorithm dependent on ERH, verify using Eichler-Selberg trace formula for cusp forms

Mosunov, J. (2014): $|\Delta| < 2^{40} (\approx 1.1 \times 10^{12})$:

- compute h_Δ unconditionally using class number formulas (power series arithmetic), resolve group structures.

Class Numbers and Sum of Three Squares

$r_3(n)$: number of integer solutions to $n = x_1^2 + x_2^2 + x_3^2$ ($n \in \mathbb{Z}^{>0}$)

Easy (classical) identity:

$$\theta_3^3(q) = \sum_{n=0}^{\infty} r_3(n) q^n$$

where $\theta_3(n) = 1 + 2\sum_{n=1}^{\infty} q^{n^2}$.

Well-known that $h_{-n} \mid r_3(n)$.

h_Δ Via Polynomial Arithmetic (Mosunov, J. 2014)

Idea: compute h_Δ for all $|\Delta| < M$ by

- computing $\theta_3^3(q) \bmod q^{M+1}$ (as power series in q).

Advantages:

- class numbers are unconditionally correct (no verification requried)
- problem reduces to multiplication of degree M polynomials (out-of-core FFT, FLINT implementation)
- compute structure of Cl_Δ by considering only primes with $p^2 \mid h_\Delta$

Problem:

- $r_3(n) = 0$ for $n \equiv 7 \pmod 8$, so use RJW method for $\Delta \equiv 1 \pmod 8$

Results

Cl_Δ for all Δ with $\Delta < 2^{40} \approx 10^{12}$ — 334211458670 fields in total

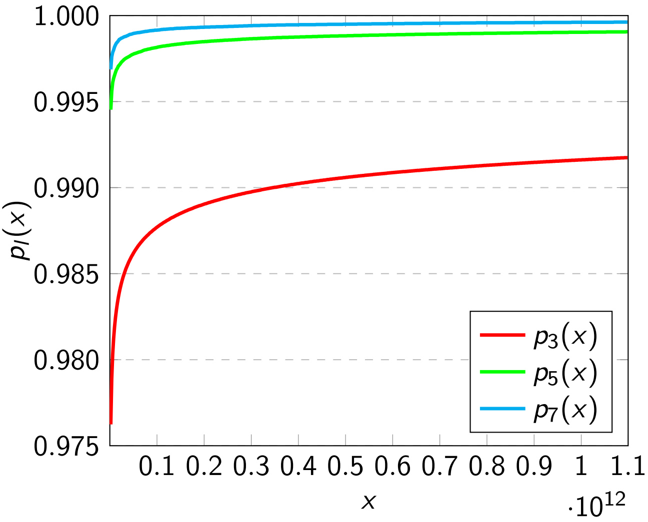
Run-time (2.67 GHz Xeon cores, 8 GB RAM each)

- $\Delta \neq 1 \pmod 8$: 258 days ($\approx$ 4 days on 64 cores)
- $\Delta \equiv 1 \pmod 8$: 1658 days ($\approx$ 2 days on 1008 cores)

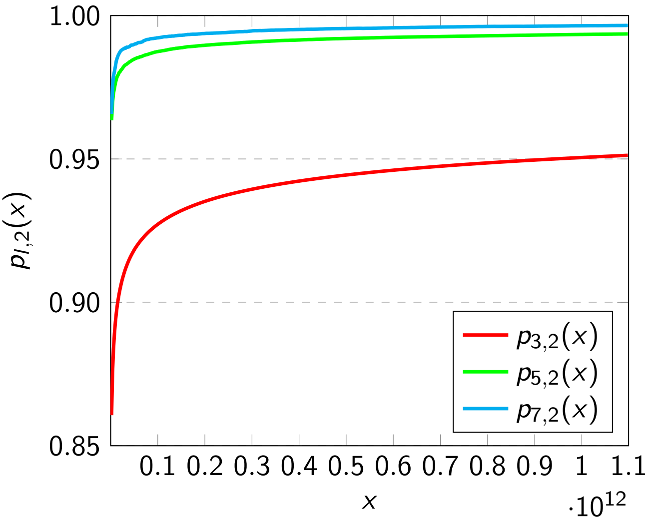
Smallest $|\Delta|$ with:

- non-cyclic $5, 7, 11$-Sylow subgroups: $\Delta = -656450533751$, $Cl_\Delta \cong C(4 \cdot 5 \cdot 7 \cdot 11) \times C(2 \cdot 5 \cdot 7 \cdot 11)$
- non-cyclic $5, 7, 17$-Sylow subgroups: $\Delta = -658234953151$, $Cl_\Delta \cong C(2 \cdot 5 \cdot 7 \cdot 17) \times C(5 \cdot 7 \cdot 17)$
- 17-rank 3 : $\Delta = -824746962451$, $Cl_\Delta \cong C(170) \times C(34) \times C(34)$

Probability that $l \mid h_\Delta$



Probability that l-rank is 2



Further work

Improving the $\Delta \equiv 1 \pmod 8$ case:

- Identity of Humbert gives one possible solution, but involves costly inversion of power series
- Investigate relationships of h_Δ with representations numbers of ternary forms other than $x_1^2 + x_2^2 + x_3^2$?

Class number formulas for $\Delta > 0$?

Other types of number fields? Cubic? Cyclotomic?