Improved Methods for Finding Imaginary Quadratic Fields with High n-rank

Michael J. Jacobson, Jr.

UNIVERSITY OF CALGARY

Joint work with C. Bagshaw, N. Rollick, and R. Scheidler

LuCaNT 2023, ICERM

Quadratic Fields

Quadratic field: $\mathbb{Q}(\sqrt{\Delta}) = \{x + y\sqrt{\Delta} \mid x, y \in \mathbb{Q}\}$

- $\Delta \equiv 0, 1 \pmod 4$: discriminant
- Δ or $\Delta/4$ is square-free (fundamental discriminant)
- $\Delta < 0$: imaginary quadratic

Cl_Δ : ideal class group (finite abelian)

- Elementary divisors: d_i such that $d_{i+1} \mid d_i$ and $Cl_\Delta \cong \prod C(d_i)$

$r_n(\Delta)$: n-rank (number of elementary divisors of Cl_Δ divisible by n)

What Do We Know about the p-Rank (p odd prime)?

Not much!

Cohen-Lenstra heuristics: $\{\Delta \mid r_p(\Delta) = k\}$ has positive natural density (approx. $1/p^{k^2}$) for all $k \geq 0$

- seems true (extensive data), not proved for a single pair (p, k).

Some infinite families known for small (p, k):

- for all n and $k = 1$ (Nagell 1922)
- for all n and $k = 2$ (Yamamoto 1970)
- $p = 3$ and $k = 3, 4$ (Craig 1977)
- $p = 5$ and $k = 2, 3$ (Mestre 1992)

Largest Known p-ranks

Question: Is the p-rank unbounded?

- no known examples with $r_p(\Delta) > 6$

$r_3(\Delta) \leq 6$	Llorente and Quer 1987 (using Diaz y Diaz 1978)
$r_5(\Delta) \leq 4$	Schoof 1983 (using Mestre 1983)
$r_7(\Delta) \leq 3$	Solderitsch 1977
$r_{11}(\Delta) \leq 3$	Léprevost 1993
$r_{13}(\Delta) \leq 3$	Ramachandran, J., Williams 2006
$r_{17}(\Delta) \leq 3$	Mosunov, J. 2016
$r_{19}(\Delta) \leq 3$	Ramachandran, J., Williams 2006

Our Results

Goal:

- construct imaginary quadratic fields with "large" p-rank
- as small discriminants as possible

Results:

- improvements to Diaz y Diaz's algorithm, generalization to odd $n > 3$
- smallest known example with $r_5(\Delta) = 4$
- first example with $r_7(\Delta) = 4$

Yamamoto 1970: $r_n(\Delta) \geq 2$

Suppose $\mathfrak{m}^n$ is principal ($\mathfrak{m}$ has order n in Cl_Δ), i.e.

$$\mathfrak{m}^n = \left(\frac{y + z\sqrt{\Delta}}{2} \right), \quad \text{for } n \in \mathbb{N},\ y, z \in \mathbb{Z}$$

Taking norms (assuming $N(\mathfrak{m}) = m$):

$$4m^n = y^2 + z^2|\Delta| \tag{1}$$

Idea: find *two* solutions with the *same* Δ and prove that

- both solutions correspond to ideal classes of order **exactly** n
- these classes are independent

Search Method (generalized and simplified Diaz y Diaz)

Want to search for integers m_1, y_1, m_2, y_2 such that

$$4m_1^n - y_1^2 = (\lambda_1^2)z^2|\Delta|$$
$$4m_2^n - y_2^2 = (\lambda_2^2)z^2|\Delta|$$

Fix λ_1, λ_2. For all m_1, m_2 such that $1 < m_2 < m_1 \leq B$:

- Rearrange and equate: $4\lambda_2^2 m_1^n - 4\lambda_1^2 m_2^n = (\lambda_2 y_1)^2 - (\lambda_1 y_2)^2$
- Factor $4\lambda_2^2 m_1^n - 4\lambda_1^2 m_2^n = ab$
- Using $ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$, set $y_1 = \frac{a+b}{2\lambda_2}$, $y_2 = \frac{a-b}{2\lambda_1}$
- If $y_1, y_2 \in \mathbb{Z}$, obtain Δ from $y_1^2 - 4m_1^n = (\lambda_1 z)^2|\Delta|$ if it is < 0

Note: Diaz y Diaz parameterizes $m_2 = m_1 + t$ with $1 \leq m_1 < m_2 < m_1^{p/2}$

Improvements

Yields two solutions to (1). To test $r_n(\Delta) \geq 2$:

- Check order n: need $c_i = \gcd(m_i, \lambda_i z) \mid \Delta$ and c_i squarefree
- Check independence: eg. if n is prime, need
  - $m_1 < \sqrt{|\Delta|/4}$, $m_2^{(n-1)/2} < \sqrt{|\Delta|/4}$, and $m_1 \nmid m_2^{(n-1)/2}$

Improvements:

1. Independence requires $m_2 < |\Delta|^{1/(n-1)}$, too restrictive for $n > 3$
   - compute ideals of norm m_1 and m_2 (extension of Kuroda 1964)
   - compute subgroup they generate
2. Sieve $f(m_1, m_2) = 4\lambda_2^2 m_1^n - 4\lambda_1^2 m_2^n$ instead of factoring each value.

Performance in Practice

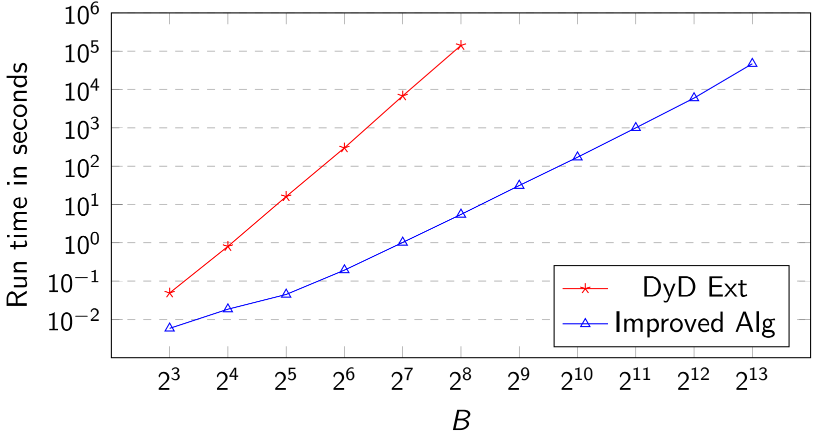

Figure: Run times for various upper bounds on m_1, for $p = 5$

Performance in Practice

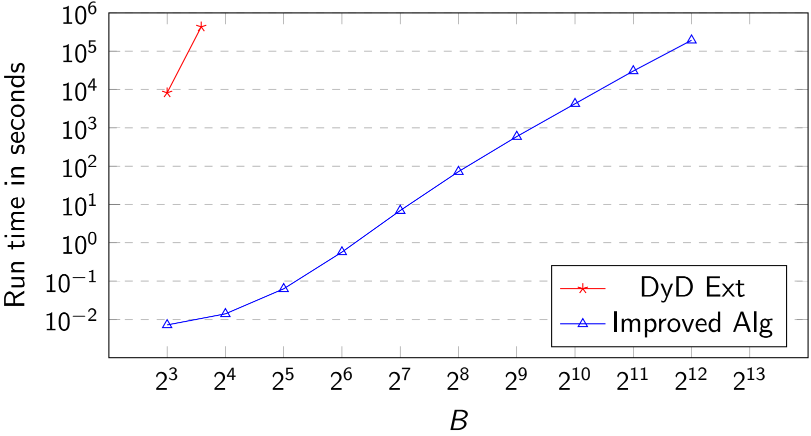

Figure: Run times for various upper bounds on m_1, for $p = 11$

Search Statistics

239 cores (2x Intel Xeon Gold 6148 CPU, 2.40GHz)

Prime	B	$\#\Delta$ found	Search t (days)	$\#Cl_\Delta$ computed	Cl_Δ t (days)
3	196608	20609841975	197.53	20609841975	1233.77
5	65536	1331448842	1452.29	1331448842	2842.37
7	40960	402708300	1689.29	297354233	3346.00
11	8192	13236853	1258.75	10342190	3346.00
13	5632	5013641	1419.18	2522501	3346.00

Observations:

- fewer examples found for larger p (as expected)
- most time is spent computing class groups

Results

p	$r_p(\Delta)$	Smallest Known	Smallest Found	# Δ Found
3	2	−3299	−3299	19465189858
3	3	−3321607	−3321607	1138191130
3	4	−653329427	−653329427	6454019
3	5	−5393946914743	−5393946914743	6968
5	2	−11199	−11199	1318152618
5	3	−11203620	−11203620	13291706
5	**4**	−258559351511807	**-1264381632596**	4518
7	2	−63499	−149519	296341915
7	3	−501510767	−16974157711	1012251
7	**4**	?	**-469874684955252968120**	**67**

$r_7(\Delta) = 4$ example:
$Cl_\Delta \cong C(340830) \times C(14) \times C(14) \times C(14) \times C(2) \times C(2) \times C(2)$

Future Work

Fast heuristic filter for large p-ranks

- Llorente and Quer 1987: use connection between 3-rank and elliptic curve rank, Birch Swinerton-Dyer to estimate rank
- Can we do this for $p > 3$?

Compare/combine with geometric methods (eg. Gillibert, Levin 2018)?

Adapt Belabas 2004 (tabulation of Δ with $r_3(\Delta) > 1$) for $p > 3$?

New ideas!?