Constructing Class Groups of Imaginary Quadratic Fields with Large *n*-Rank

Michael J. Jacobson, Jr.

UNIVERSITY OF CALGARY

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

WCNT, December 18, 2018

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)

- equivalence classes of fractional ideals modulo principal ideals

$r_n(\Delta)$: 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 imply that the set $\{\Delta \mid r_p(\Delta) = k\}$ should have positive natural density for all $k \geq 0$

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

Question: Is the p-rank unbounded?

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

$r_3(\Delta) \leq 6$	Llorente and Quer, 1988 (using Diaz y Diaz 1975)
$r_5(\Delta) \leq 4$	Schoof, 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 n-rank
- 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 (order n), 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 n
- these classes are independent

Algorithm to Produce Small Δ (improved!)

Diaz y Diaz 1974: efficient search using Yamamoto's idea for $p = 3$

- extension to arbitrary p (Rollick 2014)
- extension to arbitrary n, improved search algorithm (Bagshaw 2018)

Set-up (Bagshaw 2018):

- want to search for integers m_1, y_1, m_2, y_2 such that

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

  for $\lambda_1, \lambda_2 \in \mathbb{Z}$ (Diaz y Diaz: $\lambda_1 = \lambda_2 = 1$)
- equate and rearrange: $4\lambda_2^2 m_1^n - 4\lambda_1^2 m_2^n = (\lambda_2 y_1)^2 - (\lambda_1 y_2)^2$

Algorithm (sketch)

Fix integers $\lambda_1, \lambda_2, m_1 > 0, m_2$ such that $1 < m_2 < m_1$

1. Factor $4\lambda_2^2 m_1^n - 4\lambda_1^2 m_2^n = ab$
2. Using $ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$, set $y_1 = \frac{a+b}{2\lambda_2}$, $y_2 = \frac{a-b}{2\lambda_1}$
3. 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

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

- Check order n classes: need $c_1 = \gcd(m_1, \lambda_1 z) \mid \Delta$, $c_2 = \gcd(m_2, \lambda_2 z) \mid \Delta$ and both c_1 and c_2 square-free
- Check independence: eg. if n is prime, need
  - $m_1 < \sqrt{|\Delta|/4}$, $m_2^{(n-1)/2} < \sqrt{|\Delta|/4}$, and $m_1 \nmid m_2^{(n-1)/2}$

Results ($m_1 \leq 500$)

p	$r_p(\Delta)$	Smallest Known	Smallest Found	λ_1, λ_2
5	2	-11199	-12451	2,1
5	3	-11203620	-35663739	3,1
5	4	-258559351511807	-1264381632596	1,1
7	2	-63499	-183619	3,1
7	3	-501510767	-703668901863	3,1
7	4	?	$-46987468495525296812O$	1,1

$m_1 \leq 1700$ used for the last example

Future Work

Optimize implementation (eg. sieving to factor LHS)

Compute ideal classes instead of norm bound?

Try with methods to ensure $r_p(\Delta) \geq 3$ (Diaz y Diaz, 1978)

Larger bounds on the m_i, other p (3,11,...)

Compare with geometric methods (Mestre, Schoof, Gillibert/Levin, ...)