Contemporary Mathematics
Volume **796**, 2024
https://doi.org/10.1090/conm/796/15995

Improved methods for finding imaginary quadratic fields with high n-rank

Christian Bagshaw, Michael J. Jacobson, Renate Scheidler, and Nickolas Rollick

Abstract. We describe a generalization and improvement of Diaz y Diaz's search technique for imaginary quadratic fields with 3-rank at least 2, one of the most successful algorithms for generating many examples with relatively small discriminants, to find quadratic fields with large n-ranks for odd $n \geq 3$. An extensive search using our new algorithm in conjunction with a variety of further practical improvements produced billions of fields with non-trivial p-rank for the primes $p = 3, 5, 7, 11$ and 13, and a large volume of fields with high p-ranks and unusual class group structures. Our numerical results include a field with 5-rank at least 4 with the smallest absolute discriminant discovered to date and the first known examples of imaginary quadratic fields with 7-rank at least 4.

1. Introduction

For any positive integer n, the n-rank of a quadratic field is the number of elementary divisors of the ideal class group that are divisible by n. Computing the 2-rank of a quadratic field is no more difficult than factoring its fundamental discriminant, but much less is known about the n-rank for $n > 2$. The Cohen-Lenstra heuristics [**4**] predict that the odd part of the class group of a quadratic field is almost always cyclic and that fields with large odd n-rank are extremely rare. Nevertheless, these heuristics do imply that fields with a given n-rank should occur infinitely often for every odd integer n and rank, and moreover with a fixed, albeit small, density. However, existence has only been demonstrated for very small n and rank. Fields with n-rank exceeding 2, for n an odd prime, are known only for odd primes $n \leq 19$, and examples with n-rank exceeding 3 are only known for n equal to 3 and 5. As a result, the development of special construction and search techniques for producing quadratic fields with n-ranks exceeding 1 is a challenging and interesting problem that has undergone intense investigation for many decades (see the discussion later in this section for a wide range of references).

Constructing fields with non-trivial n-rank is also important in the context of class field theory, especially when $n = p$ is an odd prime. The number of unramified degree p extensions of a quadratic field of discriminant Δ is $(p^r - 1)/(p - 1)$, where r

Key words and phrases. Quadratic field, class group, n-rank, large scale computation.

The first two authors were supported by NSERC through USRAs. The third and fourth author are supported through NSERC Discovery Grants.

is the p-rank of $\mathbb{Q}(\sqrt{\Delta})$. Thus, quadratic fields $\mathbb{Q}(\sqrt{\Delta})$ with large p-rank give rise to large counts of such extensions, or equivalently, to large counts of degree p fields of discriminant $\Delta^{(p-1)/2}$ whose Galois closure has the dihedral group of order $2p$ as its Galois group. When $\Delta < 0$, Hilbert's Theorem 94 guarantees that for every unramified degree p extension of $\mathbb{Q}(\sqrt{\Delta})$, there exists a unique ideal class of $\mathbb{Q}(\sqrt{\Delta})$ of order p that capitulates i.e. becomes the principal class, in the extension. The principalization (or capitulation) problem in this setting asks to match all the unramified degree p extensions with their capitulating order p ideal classes. This problem is generally computationally challenging, especially in imaginary quadratic fields with high p-rank where the number of possible capitulation matches is large. Finally, the p-rank of a quadratic field determines the behaviour of its p-class tower, i.e. the tower of fields, beginning with the quadratic field itself, for which each extension is the p-Hilbert class field of the previous field. Imaginary quadratic fields with p-rank at most 1 are known to have p-class towers of finite length, and those with p-rank at least 3 have infinite p-class towers [13]. However, there are no known examples of imaginary quadratic fields with p-rank 2 and p-class tower of length at least 3, let alone infinite length [17]. Thus, efficiently constructing fields with p-rank 2 is of particular interest in computational class field theory.

Research into quadratic fields of large n-rank arguably began in 1922, when Nagel [21] proved that for any positive integer n there exist infinitely many imaginary quadratic fields whose class number is divisible by n. Kuroda [14] made Nagel's result constructive and in 1964 established a connection between solutions of certain Diophantine equations and imaginary quadratic fields whose class number is a multiple of n. Building on Kuroda's approach, research intensified in the 1970s, beginning with Yamamoto [33] who established the existence of infinitely many imaginary quadratic fields of n-rank at least 2. Craig [5, 6] discovered infinite families of imaginary quadratic fields of 3-rank 3 and 4, but the smallest[1] discriminant of his 3-rank 4 construction (listed explicitly in [9]) has 104 decimal digits. More practical constructions of quadratic fields with high 3-rank soon followed, including work of Shanks et al. [22, 26–28], Diaz y Diaz [7, 8], Buell [3], and Llorente and Quer [16]. We also note that Elkies [10] found the field $\mathbb{Q}(\sqrt{-217541503961543485618350976479})$ to have a 3-rank of 8, by using connections between 3-ranks of quadratic number fields and ranks of elliptic curves.

In contrast, there has been relatively little work on producing fields with high p-rank for $p > 3$. Solderitsch [29] used Kuroda's approach to find the first known example of an imaginary quadratic field with 7-rank equal to 3. More recently, the work of Mestre [18], Schoof [25] and Leprevost [15] departed from these classical techniques, deploying instead more sophisticated tools from algebraic geometry and the theory of elliptic curves to produce quadratic fields with large p-rank for certain small primes p. Most recently, Gillibert and Levin [11] unified many of these methods (both Diophantine and geometric) and interpreted them all through a geometric lens.

Rather than finding infinite parameterized families of fundamental discriminants defining quadratic fields of high n-rank — which is the approach taken in

[1] All the discriminants under consideration here are negative. For simplicity, without explicitly mentioning it, any size attribute used herein will refer to absolute value. For example, when we speak of discriminants that are large, small, minimal etc., we mean that their absolute value is large, small, minimal.

many of the aforementioned sources — our goal is to produce a high yield of fields with small discriminants and large n-rank, including minimal discriminants for each n. For this reason, we chose to follow Diaz y Diaz's approach [**7**, **8**] because his algorithm is extremely effective in producing a large volume of quadratic fields with 3-rank at least 2 and relatively small discriminants. Closely following the ideas of Kuroda [**14**], Diaz y Diaz searched for triples of positive integers (m, y, z) satisfying the norm equation

$$4m^3 = y^2 - z^2\Delta \tag{1.1}$$

for a fundamental discriminant $\Delta < 0$. Under certain conditions, such a triple gives rise to an ideal $\mathfrak{m}$ of norm m in the ring of integers of $\mathbb{Q}(\sqrt{\Delta})$ whose cube is principal, generated by $\alpha = (y + z\sqrt{\Delta})/2$. Thus, for fixed Δ, two such triples satisfying these conditions yield two ideals $\mathfrak{m}_1$ and $\mathfrak{m}_2$ whose cubes are principal. Additional restrictions guarantee that the classes represented by $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are independent in the class group of $\mathbb{Q}(\sqrt{\Delta})$, thereby yielding a quadratic field $\mathbb{Q}(\sqrt{\Delta})$ of 3-rank at least 2.

Our main goal is to generalize Diaz y Diaz's method of [**7**, **8**] and combine it with a new and improved search technique to generate examples of quadratic fields with discriminants of modest size and large n-ranks for arbitrary odd $n \geq 3$. In [**14**, Theorem 2] Kuroda gave sufficient conditions under which a solution (m, y, z) to

$$4m^n = y^2 - z^2\Delta \tag{1.2}$$

corresponds to an ideal class of order n in the class group of $\mathbb{Q}(\sqrt{\Delta})$. Unfortunately, to obtain two independent ideal classes of order n following Diaz y Diaz's reasoning, the conditions on the corresponding solutions of (1.2) become increasingly restrictive as n grows. An alternative approach is to check computationally whether these two ideals generate independent classes of order n. Specifically, we search for multiple solutions of (1.2) with the same discriminant Δ, compute a $\mathbb{Z}$-basis for the ideal corresponding to each solution, and finally check whether or not these ideals represent independent classes. This removes the aforementioned restrictive conditions, thereby producing a much higher yield of fields with high n-rank.

To obtain quadratic fields of 3-rank at least 2, Diaz y Diaz only considered pairs of solutions (m, y) of (1.2) for fixed Δ and z. As a further generalization of his technique, we allow z to vary. More specifically, we introduce an additional variable parameter λ and search for triples of solutions (m, y, λ) of the more general norm equation

$$4m^n = y^2 - \lambda^2 z^2\Delta \tag{1.3}$$

with Δ, z fixed. For odd primes $n = p$, this search strategy produced a higher yield of discriminants of moderate size defining quadratic fields of high p-rank compared to Diaz y Diaz's approach of only considering $\lambda = 1$. We also include a number of practical improvements designed to speed up the search for solutions of (1.3).

Although some of our theoretical results hold for arbitrary odd n (in which case this is explicitly indicated), our main focus was on odd primes $n = p$. We used our novel algorithm to carry out extensive computations searching for new examples of imaginary quadratic fields with high p-rank for the primes $p = 3, 5, 7, 11$ and 13. Overall, we found billions of fields of p-rank 2 and higher. Most noteworthy are the 67 fields of 7-rank at least 4, which represent the first known examples of fields with a 7-rank exceeding 3. Among them, the field with the smallest discriminant is $\mathbb{Q}(\sqrt{-4698746849552529681 20})$. Our numerical results also include 4518 fields of 5-rank at least 4, among which the field $\mathbb{Q}(\sqrt{-126438163259})$ has the smallest known discriminant of an imaginary quadratic field with 5-rank at least 4.

Our paper is organized as follows. The necessary mathematical framework is provided in Section 2, where we extend Kuroda's Theorem [**14**, Theorem 2] to the more general Diophantine equation (1.3) and generalize Diaz y Diaz's sufficient conditions for independence of ideal classes in [**7**, Section 3] from $n = 3$ to arbitrary odd n. We also give an explicit $\mathbb{Z}$-basis for the ideal corresponding to any solution of (1.3) which can be used to significantly speed up the independence test even when $n > 3$. In Section 3, specializing to the case $n = p$ an odd prime, we demonstrate how Diaz y Diaz's approach in [**7**,**8**] to searching for solutions to (1.1) can be extended to (1.3) and improve the associated search method to generate solutions more efficiently. In Section 4, we compare different construction techniques under multiple metrics to identify the strategy that is best suited to a large-scale computation for each prime under consideration. The results of our extensive computations searching for fields with high p-rank for the primes p with $3 \leq p \leq 13$ are presented in Section 5, with some unusual class group examples listed in an appendix. Additionally, an implementation of the main algorithms described here can be found in [**1**].

2. Mathematical Framework

Fix a fundamental discriminant $\Delta < 0$ and an odd integer $n \geq 3$. The term "ideal" will always refer to an integral ideal in the maximal order of the imaginary quadratic field $\mathbb{Q}(\sqrt{\Delta})$. In this section, we describe the relationship between solution triples (m, y, z) of (1.2) and ideals representing elements of order n in the ideal class group of $\mathbb{Q}(\sqrt{\Delta})$. For n a prime, we also provide a set of sufficient conditions for two distinct solutions of (1.2) to give rise to two independent ideal classes of order n. This extends the theory underlying Diaz y Diaz's algorithm [**7**] for finding imaginary quadratic fields of 3-rank 1 and 2 to n-ranks where n is any odd prime.

For any algebraic integer $\alpha \in \mathbb{Q}(\sqrt{\Delta})$, let $\overline{\alpha}$ denote its conjugate, $N(\alpha)$ its norm and (α) the principal ideal generated by α. We begin with the following simple observation. Let $\mathfrak{m}$ be an ideal such that $\mathfrak{m}^n$ is principal, $m \in \mathbb{Z}$ its norm, and $w = (y + z\sqrt{\Delta})/2$ a generator of $\mathfrak{m}^n$. Then taking norms of the identity $\mathfrak{m}^n = (w)$ shows that (m, y, z) is a solution of (1.2). Lemma 5 of [**7**] provides an essentially converse result in the case $n = 3$. Specifically, suppose (m, y, z) is a solution of (1.1) with $yzm \neq 0$ such that $\gcd(z, m)$ is squarefree and a divisor of Δ. Then there exists an ideal $\mathfrak{m}$ of norm m that generates an ideal class of order 3. Using Kuroda's reasoning of [**14**, Theorem 2], we generalize this result to arbitrary odd n and additionally compute an explicit $\mathbb{Z}$-basis of any such ideal $\mathfrak{m}$.

For any $a, p \in \mathbb{Z}$ with a non-zero and p prime, let

$$v_p(a) = \max\{\nu \geq 0 \mid p^\nu \text{ divides } a\}$$

denote the standard p-adic valuation. Since Δ is a fundamental discriminant, we have $v_p(\Delta) = 0$ or 1 for p odd and $v_2(\Delta) = 0$, 2 or 3, with $\Delta/4 \equiv 3 \pmod 4$ when $v_2(\Delta) = 2$.

Lemma 2.1. *Let (m, y, z) be an integer triple satisfying (1.2) with $myz \neq 0$, and assume that $c = \gcd(z, m)$ is squarefree and divides Δ. Let p be any prime divisor of m. Then the following hold.*

(a) *If p divides c, then $v_p(m) = 1$, $v_p(z) = (n-1)/2 < v_p(y)$ and p ramifies in $\mathbb{Q}(\sqrt{\Delta})$.*

(b) *If p divides m/c, then p does not divide $yz\Delta$ and p splits in $\mathbb{Q}(\sqrt{\Delta})$.*

Proof. Suppose p divides c. Then p divides Δ, so p ramifies in $\mathbb{Q}(\sqrt{\Delta})$. Since p^3 divides both m^n and $z^2\Delta$, (1.2) implies that $p^2 \mid y$.

Assume contrary to part (a) that $p^2 \mid m$. Then $v_p(z) = 1$ since c is squarefree. It follows that $v_p(4m^n) \geq 2n \geq 6$ and $3 \leq v_p(z^2\Delta) \leq 5$. This is only possible if $v_p(y^2) = v_p(z^2\Delta) = 4$, which forces $p = 2$, $v_2(y) = 2$ and $v_2(\Delta) = 2$. Dividing (1.2) by 16 yields

$$m^{n-1}\frac{m}{4} = \left(\frac{y}{4}\right)^2 - \left(\frac{z}{2}\right)^2 \frac{\Delta}{4}.$$

Since $y/4$, $z/2$ are odd and $\Delta/4 \equiv 3 \pmod 4$, the right hand side is congruent to $2 \pmod 4$ while the left hand side is divisible by 4, which is impossible. Hence $v_p(m) = 1$.

By the ultrametric inequality applied to (1.2), we now obtain

$$v_p(4m^n) \geq \min\{v_p(y^2), v_p(z^2\Delta)\}, \tag{2.1}$$

with equality if $v_p(y^2) \neq v_p(z^2\Delta)$.

Assume first that $v_p(y^2) = v_p(z^2\Delta)$. Then $p = 2$ and $v_2(\Delta) = 2$. Moreover, we have strict inequality in (2.1) since $v_2(4m^n)$ is odd whilst $v_2(y^2)$ is even. Put $k = v_2(y) = v_2(z) + 1$. Similarly to the reasoning for proving $v_p(m) = 1$, dividing (1.2) by 2^{2k} yields a right hand side that is congruent to $2 \pmod 4$. The left hand side has 2-adic valuation $n+2-2k$, so $n+2-2k = 1$, or equivalently, $k = (n+1)/2$. Together with $k = v_2(z) + 1$, this proves part (a).

Now assume that $v_p(y^2) \neq v_p(z^2\Delta)$. Then $v_p(4m^n) = v_p(z^2\Delta) < v_p(y^2)$, where the equality follows again from the fact that $v_p(4m^n)$ is odd and $v_p(y^2)$ is even. In particular, $v_p(\Delta)$ is odd and we obtain

$$2v_p(z) = n + 2v_p(2) - v_p(\Delta) = n - 1\ ,$$

as $v_p(\Delta) = 1$ when p is odd and $v_p(\Delta) = 3$ when $p = 2$. Hence $v_p(z) = (n-1)/2 < v_p(y)$ as claimed in part (a).

For part (b), note that $\gcd(c, m/c) = 1$, since $v_q(c) = v_q(m) = 1$ for primes q dividing c by part (a). Suppose p divides m/c. Then $p \nmid c$, so $p \nmid z$. Assume by way of contradiction that $p \mid y$. Then $p^2 \mid \Delta$ by (1.2), which only allows $p = 2$. Since $v_2(z^2\Delta) = v_2(\Delta) \leq 3$ and $v_2(4m^n) \geq 5$, this forces $v_2(\Delta) = 2$ and $v_2(y) = 1$. Dividing (1.2) by 4 once again yields a right hand side that is congruent to 2 (mod 4) and a left hand side that is divisible by 4, which is absurd. So $p \nmid y$, and hence $p \nmid \Delta$ by (1.2). This proves part (b). □

Recall that an ideal $\mathfrak{m}$ is primitive if no rational integer other than ±1 divides every element in $\mathfrak{m}$.

Theorem 2.2. *Let (m, y, z) be an integer triple satisfying (1.2) with $myz \neq 0$, and assume that $\gcd(m, z)$ is squarefree and divides Δ. Then there exists a primitive ideal $\mathfrak{m}$ of norm m such that $\mathfrak{m}^n = (w)$ where $w = (y + z\sqrt{\Delta})/2$.*

Proof. For brevity, put $c = \gcd(m, z)$ and $m' = m/c$. Then $\gcd(m', c) = 1$ and $c^{(n-1)/2}$ divides both y and z by Lemma 2.1. Put $w = (y + z\sqrt{\Delta})/2$ and $w' = w/c^{(n-1)/2}$. Then w and w' are algebraic integers in $\mathbb{Q}(\sqrt{\Delta})$ of respective norms m^n and $c(m')^n$. Let $\mathfrak{p}$ be a prime ideal dividing w' and p the rational prime below $\mathfrak{p}$. Then p divides c or m'. If p divides c, then $v_p(c) = 1$ and p ramifies in $\mathbb{Q}(\sqrt{\Delta})$ by Lemma 2.1. If $p \mid m'$, then p does not divide $yz\Delta$ and p splits in $\mathbb{Q}(\sqrt{\Delta})$ by Lemma 2.1. It follows that

$$(w') = \mathfrak{a}\mathfrak{b}^n \ ,$$

where $\mathfrak{a}$ is an ideal that is a product of distinct ramified prime ideals, with $\mathfrak{a}^2 = (c)$, and $\mathfrak{b}$ is an ideal of norm m' that is a product of (not necessarily distinct) prime ideals whose norms split in $\mathbb{Q}(\sqrt{\Delta})$. In particular, the principal ideal (w') is primitive.

Put $\mathfrak{m} = \mathfrak{a}\mathfrak{b}$. Then $\mathfrak{m}$ is a primitive ideal of norm $m = cm'$ and

$$\mathfrak{m}^n = \mathfrak{a}^{n-1}(w') = (c^{(n-1)/2}w') = (w) \ .$$

□

Following the terminology introduced in [**8**], we refer to the ideal $\mathfrak{m}$ of Theorem 2.2 as the ideal *corresponding* to the solution (m, y, z) of (1.2). In this same source, Diaz y Diaz gave two respective sets of sufficient conditions for the field $\mathbb{Q}(\sqrt{\Delta})$ to have 3-rank at least 1 and 2. Here we directly generalize his results to higher prime n-ranks in Proposition 2.3. For the proof, we recall that every ideal class of order distinct from 2 of $\mathbb{Q}(\sqrt{\Delta})$ contains a unique reduced ideal, and every primitive ideal of norm not exceeding $\sqrt{-\Delta/4}$ is reduced.

Proposition 2.3. *Let $\Delta < 0$ be a fundamental discriminant and $n \geq 3$ a prime.*

(a) *Let (m, y, z) be an integer triple satisfying (1.2) with $myz \neq 0$, and assume that $\gcd(m, z)$ is squarefree and divides Δ. If $1 < m < \sqrt{-\Delta/4}$, then the ideal $\mathfrak{m}$ corresponding to (m, y, z) generates a class of order n.*

(b) *Let (m_1, y_1, z_1) and (m_2, y_2, z_2) be two integer triples satisfying (1.2) with $m_1y_1z_1 \neq 0$, $m_2y_2z_2 \neq 0$, and suppose that $\gcd(m_1, z_1)$ and $\gcd(m_2, z_2)$ are both squarefree and divide Δ. If $1 < m_1 < m_2 < \sqrt{-\Delta/4}$, $m_1^{(n-1)/2} < \sqrt{-\Delta/4}$ and m_2 does not divide $m_1^{(n-1)/2}$, then the ideals $\mathfrak{m}_1$ and $\mathfrak{m}_2$ corresponding to the respective triples (m_1, y_1, z_1) and (m_2, y_2, z_2) generate independent ideal classes of order n.*

Proof. By virtue of Theorem 2.2, part (a) identifies $\mathfrak{m}$ as a reduced non-principal ideal whose n-th power is principal, so its class has order n. Similarly, in part (b), $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are distinct reduced ideals generating ideal classes of order n. Suppose these classes are dependent. Then there exists k with $1 \leq k \leq (n-1)/2$ such that $\mathfrak{m}_2$ is equivalent to $\mathfrak{m}_1^k$ or $\overline{\mathfrak{m}}_1^k$. Assume the former (the proof of the latter case is entirely analogous) and write $\mathfrak{m}_1^k = (a)\mathfrak{a}$ where $a \in \mathbb{Z}$ and $\mathfrak{a}$ is primitive. Taking ideal norms yields $N(\mathfrak{a}) \leq m_1^k < \sqrt{-\Delta/4}$, so $\mathfrak{a}$ is a reduced ideal in the class of $\mathfrak{m}_2$. It follows that $\mathfrak{a} = \mathfrak{m}_2$, so $m_1^k = a^2m_2$, contradicting the fact that m_2 does not divide $m_1^{(n-1)/2}$. □

Unfortunately, the conditions of Proposition 2.3 (b) become increasingly restrictive as n increases. It is possible to formulate analogous conditions for composite odd n, but they are even more constrained, so we do not consider this scenario. In computational experiments, we found that a search for solutions satisfying part (b) of Proposition 2.3 produces limited examples of quadratic fields of large n-rank. As an alternative strategy, we searched for solutions (m, y, z) of (1.2) satisfying Proposition 2.3 (a) and directly tested the classes generated by the corresponding ideals $\mathfrak{m}$ for independence. To facilitate this computation, we represent each such ideal $\mathfrak{m}$ by a $\mathbb{Z}$-basis which can be obtained efficiently from the solution triple (m, y, z) as follows. This, together with Theorem 2.2, could be considered stronger than a direct generalization of [**8**, Lemma B], as it describes a $\mathbb{Z}$-basis for the ideal under consideration as opposed to simply providing a basis of algebraic integers.

THEOREM 2.4. *Let (m, y, z) be an integer triple satisfying (1.2) with $myz \neq 0$, and assume that $c = \gcd(m, z)$ is squarefree and divides Δ. Put $y' = y/c^{(n-1)/2}$, $z' = z/c^{(n-1)/2}$, and define $z^* \in \mathbb{Z}$ via*

$$z'z^* \equiv \begin{cases} 1 \pmod{4m} & \text{if } z' \text{ is odd,} \\ 1 \pmod{m} & \text{if } z' \text{ is even.} \end{cases}$$

If z' is odd, put $x \in \mathbb{Z}$ via $x \equiv y'z^* \pmod{4m}$, and if z' is even, define $x \in \mathbb{Z}$ via

$$x \equiv \begin{cases} y'z^* \pmod{m}, \\ \Delta \pmod{4}. \end{cases}$$

Then $\{m, (x + \sqrt{\Delta})/2\}$ is a $\mathbb{Z}$-basis of the ideal $\mathfrak{m}$ corresponding to (m, y, z).

PROOF. By Lemma 2.1, y' and z' are integers and $\gcd(c, z') = 1$, so $\gcd(m, z') = 1$. It follows that z^* is well-defined. Dividing (1.2) by c^{n-1} yields

$$(y')^2 \equiv (z')^2\Delta \pmod{4m} \ . \tag{2.2}$$

Let $\mathfrak{c}$ be the $\mathbb{Z}$-module of rank 2 generated by m and $(x + \sqrt{\Delta})/2$. Then $\mathfrak{c}$ is an ideal if and only if $x^2 \equiv \Delta \pmod{4m}$. If z' is odd, then $(z'z^*)^2 \equiv 1 \pmod{4m}$ and $x^2 \equiv (y'z^*)^2 \pmod{4m}$, so (2.2) yields

$$x^2 \equiv (y')^2(z^*)^2 \equiv (z')^2\Delta(z^*)^2 \equiv \Delta \pmod{4m} \ .$$

Suppose now that z' is even. Then m is odd as $\gcd(z', m) = 1$, so $\gcd(m, 4) = 1$. As before, we obtain $x^2 \equiv \Delta \pmod{m}$ from (2.2). Furthermore, $x^2 \equiv \Delta^2 \equiv \Delta \pmod{4}$, since $\Delta \equiv 0$ or $1 \pmod{4}$. Thus, $x^2 \equiv \Delta \pmod{4m}$ by Chinese remaindering.

This shows that $\mathfrak{c}$ is a primitive ideal of norm m. Let $\mathfrak{m}$ be the ideal corresponding to (m, y, z). To prove that $\mathfrak{c} = \mathfrak{m}$, put $w' = (y' + z'\sqrt{\Delta})/2$. We claim that $w' \in \mathfrak{c}$. To that end, note that

$$w' = \frac{y' - xz'}{2m} m + z' \frac{x + \sqrt{\Delta}}{2} \ .$$

If z' is odd, then $xz' \equiv y' \pmod{4m}$ from the definition of x. If z' is even, then $xz' \equiv y' \pmod{m}$. In this case, m is odd, and (2.2) shows that y' is even, so again $xz' \equiv y' \pmod{2m}$ by the Chinese remainder theorem. In either case, we see that $(y' - xz')/2m \in \mathbb{Z}$, so $w' \in \mathfrak{c}$.

From the proof of Theorem 2.2, we have $\mathfrak{m} = \mathfrak{a}\mathfrak{b}$ and $(w') = \mathfrak{a}\mathfrak{b}^n$, where $\mathfrak{a}$ and $\mathfrak{b}$ are ideals such that all prime ideal factors of $\mathfrak{a}$ ramify in $\mathbb{Q}(\sqrt{\Delta})$ and all prime ideal factors of $\mathfrak{b}$ lie above split rational primes. Since $\mathfrak{c}$ divides (w'), we have $\mathfrak{c} = \mathfrak{a}'\mathfrak{b}'$ where $\mathfrak{a}'$ divides $\mathfrak{a}$ and $\mathfrak{b}'$ divides $\mathfrak{b}^n$. Taking norms of $\mathfrak{c}$ and $\mathfrak{m}$ (which both have norm m) yields $(\mathfrak{a}')^2 = \mathfrak{a}^2$ and $\mathfrak{b}'\overline{\mathfrak{b}'} = \mathfrak{b}\overline{\mathfrak{b}}$. Thus, $\mathfrak{a}' = \mathfrak{a}$, and the fact that $\mathfrak{b}$ and $\overline{\mathfrak{b}}$ are coprime forces $\mathfrak{b}' = \mathfrak{b}$, so $\mathfrak{c} = \mathfrak{m}$. □

3. Generalization and Improvement of the Diaz y Diaz Approach

The results from the previous section allow us to extend Diaz y Diaz's approach from $n = 3$ to any odd prime n. In this section, we introduce new and improved search strategies for finding solutions to (1.2) and (1.3) in this case. As mentioned previously, simple conditions can be derived to generalize Proposition 2.3 to any odd $n \geq 3$, which would then allow the results of this section to be extended to this more general setting. However, henceforth, we restrict to the case where $n = p$ is an odd prime.

3.1. Diaz y Diaz's original algorithm. We begin with a brief review of Diaz y Diaz's original algorithm [**7**,**8**], which finds small solutions of (1.1) efficiently via the following observation. Suppose we select two positive integers m_1, m_2 with $m_2 > m_1 > 1$. Put

$$t = m_2 - m_1 \ , \quad N = \frac{1}{t}(m_2^3 - m_1^3) = t^2 + 3m_1t + 3m_1^2 \ .$$

Now write $N = N'N''$ and $t = t't''$ for positive integers t', t'', N', N'', and let $y = t'N' - t''N''$. If $y^2 - 4m_1^3 < 0$, we write this quantity in the form $y^2 - 4m_1^3 = z^2\Delta$ where $\Delta < 0$ is a fundamental discriminant and $z \in \mathbb{Z}$. A simple symbolic computation reveals that (m_1, y, z) and $(m_2, y + 2t''N'', z)$ are solutions of (1.1).

This approach was used by Diaz y Diaz to produce hundreds of thousands of quadratic fields with 3-rank at least 2. A very promising aspect of this technique is that many of the discriminants it produced turned out to define quadratic fields of 3-rank exceeding 2, as seen via computing their corresponding class groups. The high yield of this method motivated our generalization to arbitrary odd prime n-ranks.

Diaz y Diaz's idea for efficiently generating solutions of (1.1) directly generalizes to finding solutions of (1.2) for any odd prime $n = p$. As before, select two positive integers m_1 and m_2 with $m_2 > m_1 > 1$ and put $m_2 - m_1 = t$ and $N = (m_2^p - m_1^p)/t$. Again, write $N = N'N''$ and $t = t't''$ for positive integers t', t'', N', N'', and let $y = t'N' - t''N''$. If $y^2 - 4m_1^p < 0$, write $y^2 - 4m_1^p = z^2\Delta$ where $\Delta < 0$ is a fundamental discriminant. Then (m_1, y, z) and $(m_2, y + 2t''N'', z)$ are solutions of (1.2), and if they satisfy the conditions of Proposition 2.3, then Δ is the discriminant of a quadratic field of p-rank at least 2. The overall search procedure consists of looping over a given range of values for m_1 and, for each m_1, looping over a range of suitable t values, recording all such discriminants Δ found in this manner.

The only part of the algorithm that requires additional explanation is the range of values chosen for t (the difference between m_1 and m_2). A range of values for m_1 is selected, and for each value of m_1 we loop over all values of t such that $1 \leq t < m_1^{p/2} - m_1$. That is, we loop over values of m_2 such that $m_1 < m_2 < m_1^{p/2}$. For $p = 3$ this was the search space used by Diaz y Diaz in [**7**]. The justification for the upper bound is as follows: In order to satisfy Proposition 2.3, we need both solutions (m_1, y, z) and $(m_2, y + 2t''N'', z)$ to satisfy $m_1, m_2 < \sqrt{|\Delta|/4}$. But since $m_1 < m_2$, the condition $m_2 < \sqrt{|\Delta|/4}$ is sufficient. Combining this with the identity $4m_1^p = y^2 + z^2|\Delta|$ (which implies $|\Delta| \leq 4m_1^p$) gives $m_2 < \sqrt{|\Delta|/4} \leq \sqrt{4m_1^p/4} = m_1^{p/2}$.

3.2. Algorithmic Improvements. Although Diaz y Diaz's method was used very successfully for $p = 3$, including by Llorente and Quer [**16**] to find fields with the largest known 3-ranks, it does not scale well for larger p. The main reason is that the upper bound $m_1^{p/2} - m_1$ on t grows exponentially with p, resulting in a search space that grows too quickly. Furthermore, larger pairs (m_1, m_2) often yield larger values of Δ. Thus, to find small discriminants, it is better to exhaust smaller pairs (m_1, m_2) before moving to larger ones. We have devised a number of algorithmic improvements to the search procedure to address this issue.

Extending and Simplifying the Search Procedure. Diaz y Diaz's method finds solution pairs of (1.2) with the same z-value. We extend the search space by searching for solutions to the sightly more general pair of equations

$$\begin{aligned} 4m_1^p &= y_1^2 - \lambda_1^2 z^2 \Delta \ , \\ 4m_2^p &= y_2^2 - \lambda_2^2 z^2 \Delta \ . \end{aligned} \tag{3.1}$$

By varying λ_1 and λ_2, we can find many new solutions of (3.1) for the same values of m_1 and m_2 without greatly increasing the sizes of the discriminants.

Diaz y Diaz's search technique can be generalized to find solutions of (3.1), but there is a simpler, more efficient approach. Fix positive integers m_1, m_2, λ_1 and λ_2. We first seek integers y_1 and y_2 satisfying

$$4\lambda_2^2 m_1^p - 4\lambda_1^2 m_2^p = (\lambda_2 y_1)^2 - (\lambda_1 y_2)^2 \ .$$

If we suppose the left-hand side is factored as ab for $a, b \in \mathbb{Z}$, then since $ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$, we can set

$$y_1 = \frac{a+b}{2\lambda_2} \ , \quad y_2 = \frac{a-b}{2\lambda_1} \ .$$

If $2\lambda_2$ divides $a + b$ and $2\lambda_1$ divides $a - b$, then y_1 and y_2 are integers, so we obtain the two solutions

$$\left(m_1, \frac{a+b}{2\lambda_2}, \lambda_1 z\right) \ , \quad \left(m_2, \frac{a-b}{2\lambda_1}, \lambda_2 z\right)$$

of (3.1), where we obtain z and Δ simply by setting $\lambda_1 z^2 \Delta = y_1^2 - 4m_1^p$. By selecting values for λ_1 and λ_2 and looping over pairs of values for m_1 and m_2, this provides a systematic way of generating many solutions of (3.1). For a given tuple $(m_1, m_2, \lambda_1, \lambda_2)$, this approach also only requires one factorization, while a direct extension of Diaz y Diaz's approach would require two.

Our third improvement to the search is that instead of searching over all pairs (m_1, m_2) with $m_1 < m_2 < m_1^{p/2} - m - 1$ for some specificed range of m_1 values as described above in Section 3.1, we consider (m_1, m_2) such that $1 < m_2 < m_1$. This addresses the issue of preferring to exhaust small pairs (m_1, m_2) before moving on to larger ones, because the discriminants produced are smaller. The effect in practice is that the time required to process each potential solution of (3.1) is reduced, but we also found that our search space yielded more solutions despite the fact that the number of pairs considered is reduced.

Explicit Independence Testing. As mentioned earlier, the conditions on m_2 in Proposition 2.3 (b) required to achieve the independence of the ideal classes corresponding to simultaneous solutions of (3.1) become increasingly restrictive as p grows, thereby greatly limiting the solutions that can be found. Instead of forcing

m_2 to be small to guarantee independence, we remove the bound on m_2 and instead apply a computation to check independence, using the $\mathbb{Z}$-basis of Theorem 2.4.

For each solution (m, y, λ, z) of (3.1) found, we store the corresponding ideal and sort the ideals by discriminant. Following our search, we test for each discriminant Δ whether the set of solutions attached to Δ is sufficient to guarantee that $\mathbb{Q}(\sqrt{\Delta})$ has p-rank at least k for some integer k. It suffices to test whether the ideal classes found in this way generate a subgroup of the ideal class group of $\mathbb{Q}(\sqrt{\Delta})$ that is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^k$. To determine k, we simply compute the subgroup of the class group generated by the ideals corresponding to each solution by computing all the powers up to exponent $(p-1)$ of each ideal and then all possible products formed by these powers. This improvement has the additional benefit that multiple searches can be performed using different pairs (λ_1, λ_2). Then all the solutions for a given discriminant Δ can be combined and tested for independence as described above.

In practice, it was found that the set of solutions rarely detected that $k > 2$, even in cases when the actual p-rank of $\mathbb{Q}(\sqrt{\Delta})$ exceeded 2. Thus, when running a large-scale computation, we simply kept track of all discriminants yielding $k \geq 2$.

With this in mind, we handled the case $p = 3$ somewhat differently. Cyclic subgroups of order 3 in the class group contain the principal class and two other classes of order 3, each containing a unique reduced ideal of the same norm. Thus, in the case $p = 3$, if all solutions found correspond to reduced ideals, then one only needs to keep track of their norms: if at least two solutions correspond to ideals of different norms, then we can conclude $k \geq 2$. In a large-scale computation, this can save both time and storage. Checking whether an ideal is reduced by checking that its norm is at most $\sqrt{-\Delta/4}$ is not be very restrictive in practice, and thus we have opted for this method in the case $p = 3$.

Factoring. A final point that needs to be addressed is the factoring involved in the algorithm. Fix an odd prime p and an integer pair (λ_1, λ_2). For brevity, put $N(X, Y) = 4\lambda_2 X^p - 4\lambda_1 Y^p \in \mathbb{Z}[X, Y]$. We must then find the divisors of $N(m_1, m_2)$, which becomes increasingly time-consuming as p and m_1 get large. To improve the performance of this part of the search algorithm, we experimented with using a sieve to find small prime factors of these numbers. The main idea is as follows. For a fixed value of m_1 and every prime q less than some sieving bound, we find all values of m_2 with $2 \leq m_2 < m_1$ such that $\lambda_2^2 m_1^p - \lambda_1^2 m_2^p$ is divisible by q, using a process analogous to the Sieve of Erathosthenes. To that end, we compute the roots of $x^p - (\lambda_2/\lambda_1)^2 \equiv 0 \pmod{q}$ for each prime q. Then each value of $r \equiv x m_1 \pmod{q}$, where x is any of these p-th roots, yields a quantity $N(m_1, r)$ that is divisible by q, and the m_2 values with $N(m_1, m_2)$ divisible by q have the form $m_2 = r + kq$ for $k \in \mathbb{Z}$. After sieving in this way, we obtain for fixed m_1, λ_1, λ_2 all the primes up to the sieving bound that divide $N(m_1, m_2)$ for all m_2 with $2 \leq m_2 < m_1$. These primes are divided out of each $N(m_1, m_2)$ found and the result is factored using Sage's built-in `factor` method. Our sieve method is described in Algorithm 3.1. The same procedure is performed for all $m_1 \geq 3$ up to some suitable upper bound on m_1.

Complete Algorithm. Our complete algorithm, incorporating the improvements described above, is presented in Algorithm 3.2.

Algorithm 3.1 Factoring Sieve

Input:
- Odd prime p;
- Fixed integer m_1;
- Largest prime to sieve over, `sieve_bound`
- Integer pair (λ_1, λ_2)
- A dictionary, `roots`, containing for each prime q up to `sieve_bound`, the roots of $x^p - (\lambda_2/\lambda_1)^2 \equiv 0 \mod q$. Below "**for** $q \in$ `roots`" refers to looping over the keys in the dictionary.

Output:
- An array, `factor_array`, consisting of small prime factors of $N(m_1, m_2)$ for pairs $(m_1, 2)$, $(m_1, 3)$, $\ldots$, $(m_1, m_1 - 1)$.

```
factor_array ← []
for $m_2 \in \{0, 1, 2, \ldots, m_1 - 1\}$ do
    factor_array$[m_2] = []$
for $q \in$ roots do
    for $x \in$ roots$[q]$ do
        for $m_2 \in \{2, 3, \ldots, m_1 - 1\}$ with $m_2 \equiv x m_1 \pmod{q}$ do
            add $q$ to factor_array$[m_2]$
return factor_array
```

4. Evaluation and Parameter Selection

We performed a series of benchmarking experiments to compare the performance of Diaz y Diaz's method and its natural extension to $p > 3$ as outlined in Section 3.1 (referred to below as "DyD Ext") and our new Algorithm 3.2 (refered to as "Improved Alg"). We also evaluated the effect of each of our proposed improvements and ran tests to find suitable values of λ_1 and λ_2 to maximize the effectiveness of our search. Our findings are summarized below.

The purpose of these algorithms is not only to obtain many fields with p-rank 2, but also to help discover fields with higher p-rank. In order to identify these, we computed the class groups of as many of the fields found as was feasible. Unfortunately, there is no known algorithm to determine the p-Sylow subgroup or even the p-rank of the class group asymptotically faster than just computing the entire class group. The fastest known algorithm for computing class groups is subexponential in $\log |\Delta|$ [**12**, Theorem 13.11], but the output is only correct assuming the Generalized Riemann Hypothesis (GRH). Unconditional verification is possible but can only be done in exponential time, rendering the computation infeasible for many of the fields produced by our methods. Even computing class numbers assuming the GRH is slow compared to our search methods. Thus, we also considered the smallest discriminant produced and the overall yield of small discriminants as part of our evaluation.

Our algorithms were implemented in SageMath v. 8.8 [**32**], and the computations were performed on the University of Calgary's ARC cluster (running CentOS 7). The cluster's cpu2019 partition was used, allowing us to run simultaneous computations in parallel on up to 240 cores (2x Intel Xeon Gold 6148 CPU, 2.40GHz). When run, we allocated each core 1GB of RAM. Our code is available in a repository on GitHub [**1**].

4.1. Algorithm Comparisons.

Our first set of experiments consisted of running each of the search algorithms with the primes p with $3 \leq p \leq 13$, starting at

Algorithm 3.2 Expanded Search With Explicit Independence Testing (Improved Alg)

Input:
- Odd prime p;
- Set of integer pairs $\{(\lambda_{i,1}, \lambda_{i,2})\}$, `lambda_pairs`;
- Lower bound on m_1, `lower_`m_1;
- Upper bound on m_1, `upper_`m_1;

Output:
- A list D consisting of discriminants, each corresponding to a non-empty set of triples $\{(m_i, y_i, \lambda_{i,j} z_i)\}$ satisfying Proposition 2.3 (a) for $n = p$ with `lower_`$m_1 \leq m_1 \leq$ `upper_`m_1 and $2 \leq m_2 < m_1$, whose corresponding ideals generate a subgroup of the ideal class group of $\mathbb{Q}(\sqrt{\Delta})$ isomorphic to $(\mathbb{Z}/p\mathbb{Z})^k$ for some $k \geq 2$.

```
1:  ideals ← {}
2:  D ← []
3:  for $\lambda_1, \lambda_2 \in$ lambda_pairs do
4:      for $m_1 \in \{$lower_$m_1, \ldots,$ upper_$m_1\}$ do
5:          for $m_2 \in \{2, \ldots, m_1 - 1\}$ do
6:              $N \leftarrow 4\lambda_2^2 m_1^p - 4\lambda_1^2 m_2^p$
7:              for $a \in \{l \in \mathbb{Z}^{\geq 0} \mid l$ divides $N$ and $l \leq \sqrt{N}\}$ do
8:                  $b \leftarrow N/a$
9:                  if $2\lambda_2 \mid a + b$ then
10:                     $y_1 \leftarrow (a+b)/(2\lambda_2)$
11:                     if $y_1^2 - 4m_1^p < 0$ then
12:                         $\Delta \leftarrow$ squarefree part of $y_1^2 - 4m_1^p$
13:                         if $\Delta \not\equiv 1 \pmod 4$ then
14:                             $\Delta \leftarrow 4\Delta$
15:                         if $\Delta \mid y_1^2 - 4m_1^p$ then
16:                             $z \leftarrow \sqrt{(y_1^2 - 4m_1^p)/\Delta}$
17:                             $c_1 \leftarrow \gcd(m_1, z)$
18:                             if $c_1 \mid \Delta$ and $4 \nmid c_1$ then
19:                                 if $p = 3$ and $m_1 < \sqrt{-\Delta/4}$ then
20:                                     add $m_1$ to ideals$[\Delta]$
21:                                 if $p > 3$ then
22:                                     $x \leftarrow$ as described in Theorem 2.4
23:                                     add $[m_1, (x + y_1\sqrt{\Delta})/2]$ to ideals$[\Delta]$
24:                 if $2\lambda_1 \mid a - b$ then
25:                     $y_2 \leftarrow (a-b)/(2\lambda_1)$
26:                     Repeat Lines 11–23 using $(y_2, m_2)$ in place of $(y_1, m_1)$
27: for $\Delta \in$ ideals do
28:     if $p = 3$ then
29:         add $\Delta$ to $D$ if there are at least 2 distinct elements in ideals$[\Delta]$
30:     if $p > 3$ then
31:         add $\Delta$ to $D$ if $\langle$ideals$[\Delta]\rangle \cong (\mathbb{Z}/p\mathbb{Z})^k$ for some $k \geq 2$
32: return D
```

`lower_`$m_1 = 3$ and with data being recorded at values of `upper_`m_1 at increasing powers of 2. For a direct comparison with the Diaz y Diaz method, we only used $\lambda_1 = \lambda_2 = 1$ in Algorithm 3.2.

In all cases, our improved algorithm was significantly faster than the Diaz y Diaz method in terms of both actual run time and run time per unique field with p-rank two found. Figure 4.1 shows the runtimes for $p = 3$, Figure 4.2 shows the runtimes per p-rank two field found for $p = 3$, and Figure 4.3 shows the runtimes for $p = 11$. The time per discriminant plot is not included for $p = 11$, as no discriminants were found using DyD Ext. The results for $p = 5, 7, 13$ were analogous.

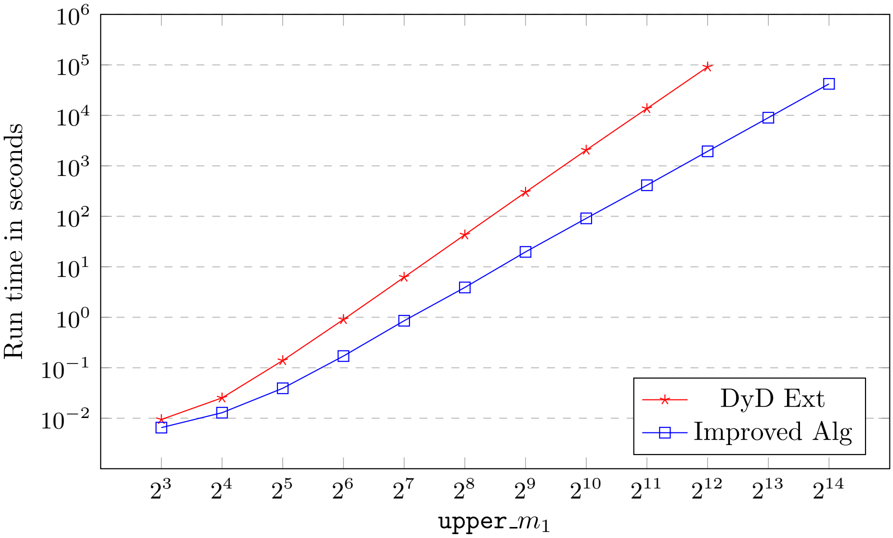

FIGURE 4.1. Run times of DyD Ext and Improved Alg for various upper bounds on m_1, for $p = 3$

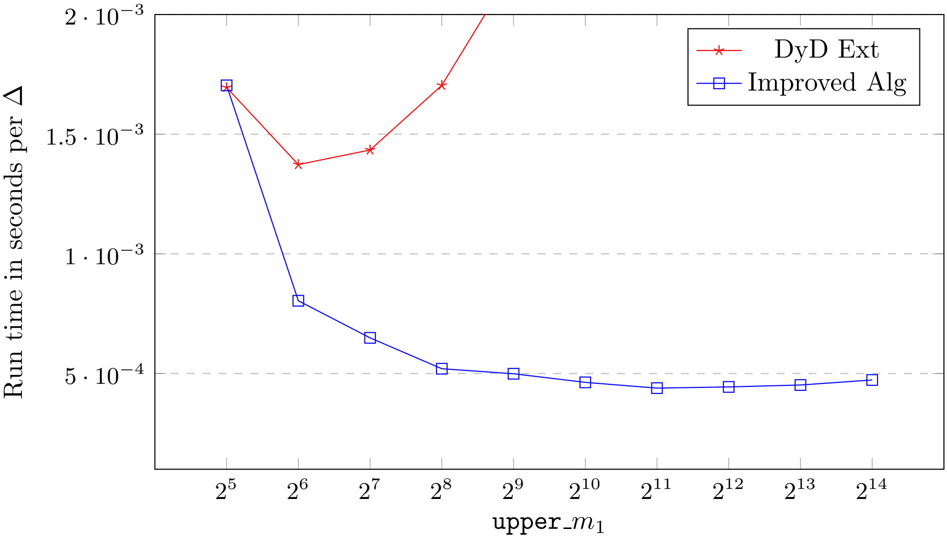

FIGURE 4.2. Run times per discriminant for DyD Ext and Improved Alg for various values of upper_m_1, for $p = 3$

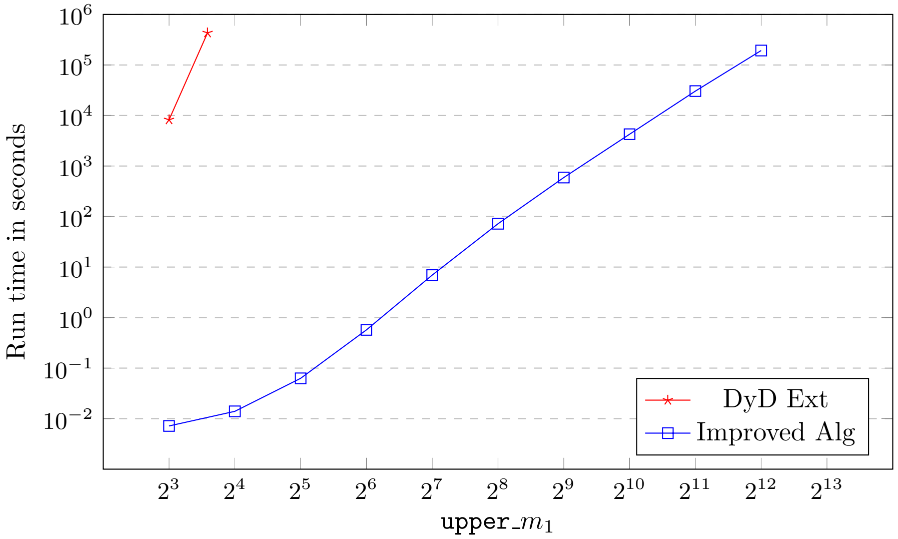

FIGURE 4.3. Run times of DyD Ext and Improved Alg for various upper bounds on m_1, for $p = 11$

Table 4.1 lists the minimal discriminant found by each algorithm, and the entry is left blank if no discriminants were found. Note that as predicted, the new algorithm, in addition to being faster overall, is more effective at finding solutions to (3.1) and, moreover, that the discriminants produced are smaller.

TABLE 4.1. Discriminants of minimal absolute value found by DyD Ext and Improved Alg for $p = 3, 5, 7, 11, 13$

			p		
Algorithm	3	5	7	11	13
DyD Ext	-3299	-53079	-5882719		
Improved Alg	-3299	-11199	-2096648	-15733605544	-9551516316168

4.2. Effect of Sieving. Our next experiments were designed to evaluate the effect of using a sieve to factor the values of $N(m_1, m_2)$ as described in Algorithm 3.1.

We first determined an appropriate bound for the sieving primes (referred to as `prime_bound` in Algorithm 3.1) experimentally as follows. We computed the total time it takes to factor all the given values of $N(m_1, m_2)$ for m_1 between certain values of lower_m_1 and upper_m_1, using assistance from Algorithm 3.1 for different values of `prime_bound`, and also without using Algorithm 3.1 (just deploying Sage's `factor` function). We choose upper_m_1 in increasing powers of 2 and let lower_m_1 = upper_$m_1 - 100$. We did this for the pair $(\lambda_1, \lambda_2) = (1, 1)$, as the optimal prime bounds should be very similar for other pairs (λ_1, λ_2).

For $p = 3, 11, 13$, we chose values of `prime_bound` in increasing powers of 2, from 2^8 to 2^{21}. We chose values of upper_m_1 starting from 2^9, up to 2^{17} for $p = 3$ and 2^{16} for $p = 11$ and $p = 13$. The dictionary containing `roots` was pre-computed for primes up to 2^{16} but this took under 2 minutes for each p. Unfortunately, factoring the values of $N(m_1, m_2)$ for these primes was always faster without the assistance of Algorithm 3.1. For $p = 3$, we suspect that this is because the quantities $N(m_1, m_2)$ are relatively small and can thus be handled easily by Sage's `factor` function, or perhaps it is due to the fact that our sieve was implemented in a high-level language without optimizations that are typically done in a C implementation. Regardless, there is surely potential for improvement in this area.

For $p = 5$ and $p = 7$, assistance from Algorithm 3.1 showed an improvement in factoring time with the right selection of `prime_bound`. Table 4.2 displays, for $p = 5$ and 7, and for different ranges of values of upper_m_1, the unassisted factoring time, the sieve-assisted factoring time and its associated value of `prime_bound`. All times are in seconds.

Table 4.2. Comparison of assisted and unassisted factoring times (in seconds) for different ranges of values of upper_m_1

					$p = 5$			
upper_m_1	512	1024	2048	4096	8192	16384	32768	65536
unassisted factoring	2.69	8.03	22.99	65.61	233.88	661.41	1734.83	5528.90
assisted factoring	6.55	16.81	40.99	98.83	261.36	642.81	1628.91	4924.33
optimal `prime_bound`	512	1024	2048	8192	8192	131072	262144	524288
					$p = 7$			
upper_m_1	512	1024	2048	4096	8192	16384	32768	65536
unassisted factoring	10.40	47.08	179.66	583.81	1890.67	5153.09	13491.52	34018.69
assisted factoring	9.93	38.98	165.13	570.21	1818.32	4506.21	12113.02	31163.75
optimal `prime_bound`	512	1024	2048	8192	262144	524288	524288	524288

4.3. Choosing Parameters for the Expanded Search. Our next experiments were designed to examine the effect of varying the parameters λ_1 and λ_2 of Algorithm 3.2, in order to determine parameter choices for our large-scale search that were most likely to yield favorable results.

To determine suitable choices, we ran experiments incrementally, testing the benefit of adding any new such pairs to the search after starting with $\lambda_1 = \lambda_2 = 1$. As an example, we provide the data from our experiments for $p = 11$ in Table 4.3 Results for $p = 3, 5, 7, 13$ were mostly analogous, with notable differences discussed below. Each line in the table corresponds to a run of our new algorithm (Algorithm 3.2) on input the pairs (λ_1, λ_2) listed in the first two columns of that line and all the lines above it. This approach quantifies the computational value of adding a new pair (λ_1, λ_2). All experiments were run with lower_$m_1 = 3$.

Columns 3 and 4 in Table 4.3 list the smallest and the median discriminant found in any given run. The remaining column headers signify the following data:

- *new* Δ lists the number of discriminants reported by Algorithm 3.2 to have p-rank at least 2 that were not found in the previous run corresponding to the row above;
- *s per new* Δ is the relative run time increase for all new discriminants, i.e. the ratio of the additional time taken (in seconds) compared to the previous row, divided by *new* Δ;

An obvious trend that we observed for all primes is that adding new pairs (λ_1, λ_2) enables Algorithm 3.2 to find smaller discriminants defining fields with p-rank at least 2. For $p = 3$ and 5, the respective provably minimal discriminants

TABLE 4.3. Incrementally adding pairs (λ_1, λ_2) for $p = 11$, $\texttt{upper\_}m_1 = 512$

λ_1	λ_2	min Δ	median Δ	new Δ	s per new Δ
1	1	-15733605544	-2409316885097325501591366943	8778	0.067515
2	1	-15733605544	-1800413784996102890457052303	4417	0.207770
1	2	-185328519	-1551091754615407644328306939	1374	0.435184
1	3	-185328519	-1364091056871805689771941779	695	0.828320
3	1	-70565939	-1007073149417658049440905299	4360	0.227851
4	1	-70565939	-816946052154444502485125447	2516	0.415843
3	2	-70565939	-795797521072323671302410443	1068	0.880585
2	3	-70565939	-780705253163238322892621827	424	1.537410
1	4	-70565939	-760023844628486720926728387	301	1.887791
1	5	-70565939	-741729080835893769769496423	265	2.147148
5	1	-70565939	-618772757856319584170735560	2850	0.351154
6	1	-70565939	-564683504170411558007215723	1051	0.918917
5	2	-70565939	-540413837611003533378344227	805	1.216898
4	3	-70565939	-533568062381971324849963279	621	1.474324
3	4	-70565939	-526707431576602266767546552	224	3.118813
2	5	-70565939	-518991454188667796823702339	149	4.069647
3	5	-70565939	-512906661353959435015354916	230	2.777062
5	3	-70565939	-492701289613950876504147715	668	1.393279
7	1	-70565939	-438924627629964845075394724	2202	0.449065
8	1	-126407	-400133798411797736175242571	1468	0.717999
5	4	-126407	-397916586199033278442104835	314	2.803772
4	5	-126407	-394450906589853749463160687	188	3.792223
9	1	-126407	-359749231801531908064767095	1345	0.783479
10	1	-126407	-341203318897141258313638135	715	1.314428

-3299 and -11199 were found just with the initial pair $(\lambda_1, \lambda_2) = (1, 1)$. But for larger primes, adding new pairs (λ_1, λ_2) generated significantly smaller discriminants. For example, for $p = 11$, the pair $(\lambda_1, \lambda_2) = (1, 1)$ produced the rather large minimal discriminant -15733605544. Adding just the pairs $(\lambda_1, \lambda_2) = (2, 1)$ and $(1, 2)$ already found a much smaller minimal discriminant, and by the time all the pairs up to $(\lambda_1, \lambda_2) = (8, 1)$ were included in the search, the algorithm discovered the significantly smaller discriminant -126407. Moreover, for all primes under consideration, the median discriminant decreased as more such pairs were added. This is highly desirable and represents convincing evidence in support of the effectiveness of our new approach to searching for solutions of (3.1) with varying pairs (λ_1, λ_2), rather than restricting to the original Diaz y Diaz setting $(\lambda_1, \lambda_2) = (1, 1)$ in [**8**].

It is also clear that adding new pairs (λ_1, λ_2) increases the yield of discriminants as p increases. However, while it is evident that adding more pairs (λ_1, λ_2) to the search appears generally favourable, it is more difficult to ascertain how many such pairs should be included and how to choose the specific pairs that bring the most benefit. Our data show that the processing time per discriminant increases as more pairs (λ_1, λ_2) are added, but the median discriminant, and often the minimal discriminant, decrease. The choice of pairs (λ_1, λ_2) to include is governed by how one wishes to balance these two factors. One noticeable trend is that pairs with

$\lambda_2 = 1$ seem to give higher yields than those with larger λ_2 values. This can be seen by their higher yields of new discriminants and relatively low seconds per new discriminant values. It is also clear that for larger primes, adding new (λ_1, λ_2) pairs has a greater impact on the minimal discriminant found. In our implementation we compute class groups, so small median discriminants are very beneficial and more (λ_1, λ_2) pairs should be chosen for larger primes. With so many factors to weigh, there is no clear strategy for selecting (λ_1, λ_2) pairs. We opted to make the following choices for a large-scale computation:

- For $p = 3$, the pairs $(\lambda_1, \lambda_2) = (1, 1), (2, 1), (3, 1)$ were chosen, as they seem to produce a high yield of discriminants at a very low cost per discriminant ("s per new Δ" value).
- For $p = 5$, the pairs $(\lambda_1, \lambda_2) = (1, 1), (2, 1), (3, 1), (4, 1), (5, 1), (1, 2)$ were chosen.
- For $p = 7$, we decided to pick the top 10 pairs with the lowest cost per discriminant, which are $(\lambda_1, \lambda_2) = (1, 1)$, $(2, 1)$, $(1, 2)$, $(3, 1)$, $(4, 1)$, $(5, 1)$, $(6, 1)$, $(7, 1)$, $(8, 1)$, $(9, 1)$.
- For $p = 11$ and $p = 13$, discriminants need to be kept small in order to compute class groups efficiently. Thus, the focus of a large-scale computation for these primes was not to search up to a large value of $\texttt{upper\_}m_1$, but rather, to search over as many (λ_1, λ_2) pairs as possible for a smaller value of $\texttt{upper\_}m_1$.

4.4. Summary. Table 4.4 lists the preferred factoring algorithm for each prime p as well as the parameters used as input to Algorithm 3.2 for a large-scale computation, based on the results of our experiments described above.

TABLE 4.4. Parameters for large-scale computation

Prime	Factoring	(λ_1, λ_2) pairs	$\texttt{upper\_}m_1$
3	Sage	(1,1), (2,1), (3,1)	196608
5	Algorithm 3.1	(1,1), (2,1), (3,1), (4,1), (5,1), (1,2)	65536
7	Algorithm 3.1	(7,1), (8,1), (9,1), (1,2)	40960
11	Sage	(λ_1, λ_2) with $1 \leq \lambda_1, \lambda_2 \leq 10$ and $\gcd(\lambda_1, \lambda_2) = 1$; (63 total pairs)	8192
13	Sage	Same as for $p = 11$	5632

Factoring $N(m_1, m_2)$ for $p = 3, 11, 13$ was completed unassisted using Sage's `factor` function. For $p = 5$ and 7 we used sieving to partially factor these values as described in Section 4.2. For our implementation, we fit the data in Table 4.2 to curves, one for $p = 5$ and another for $p = 7$, and used these curves to compute a value of $\texttt{prime\_bound}$ for values of $\texttt{upper\_}m_1$ not occurring in the table. For $p = 5$ we used

$$\texttt{prime\_bound} = 2e^{1.8(\log_2(\texttt{upper\_}m_1)-9)}$$

and for $p = 7$ we determined

$$\texttt{prime\_bound} = 50e^{1.3(\log_2(\texttt{upper\_}m_1)-7)} \quad .$$

5. Numerical Results

In this section we describe the results of our final searches for imaginary quadratic fields whose class groups have large p-ranks for $p = 3, 5, 7, 11$ and 13. All searches were run with $\texttt{lower\_}m_1 = 3$, using the algorithms and parameters listed in Table 4.4. The $\texttt{upper\_}m_1$ values were chosen to be as large a power of 2 (or a sum of large powers of 2) as possible so that searches could be run in roughly a week on 239 cores running simultaneously. The exception is for $p = 3$, where searches needed to be halted due to storage capacity.

Run time data are presented in Table 5.1, which lists the total run time and number of discriminants found for each prime. Class groups were computed using PARI/GP's quadclassunit [**31**, Section 3.8.88] with the discriminants distributed over the 239 compute nodes. This function implements the subexponential algorithm mentioned in Section 4, and since the correctness of this algorithm requires the assumption of the GRH, our p-ranks are only exact under the GRH as well. However, the method does compute generators of each independent cyclic subgroup of the class group and verifies that each has the correct order, so the p-ranks claimed here are unconditionally lower bounds on the true p-ranks.

Computations were halted if not all class groups were found after 2 weeks of real-time computing. "#Δ found" refers to the total number of discriminants found in the search. "Search t" refers to the total time (in days) it took to run the search. "#Class groups computed" refers to the number of discriminants for which class groups were computed, and "Class group t (days)" refers to the total time taken to compute these class groups. The times given are total CPU time taken over all 239 nodes. Note that, as expected, class group computation is in most cases the bottleneck with these computations. For all primes except 3 and 5, the search methods produced far more fields with p-rank at least 2 than we were able to compute class groups.

Table 5.1. Final counts and times

Prime	#Δ found	Search t (days)	#Class groups computed	Class group t (days)
3	20609841975	197.53	20609841975	1233.77
5	1331448842	1452.29	1331448842	2842.37
7	402708300	1689.29	297354233	3346.00
11	13236853	1258.75	10342190	3346.00
13	5013641	1419.18	2522501	3346.00

Table 5.2 breaks down the p-ranks of all discriminants whose class groups were computed. "Previous* Min Δ" refers to the previously found smallest discriminant corresponding to that p-rank; if no proof of minimality was provided for this discriminant in the literature, the entry is marked with an asterisk (*). The proved minimal discriminants for each p-rank were found in [**20**], aside from the proved minimum for 3-rank 5 which was found in [**2**] and the previous minimal 5-rank 4 example (identified with a *) was found in [**25**]. If no discriminant of that p-rank had previously been found, that entry is left blank. "Min Δ found“ refers to the minimal discriminant found with that p-rank in our computations, and "#Δ found" refers to the number of discriminants found in our computations corresponding to that p-rank.

Table 5.2. p-rank results

p-rank	Previous* Min Δ	Min Δ found	# Δ found
3-rank ≥ 2	-3299	-3299	19465189858
3-rank ≥ 3	-3321607	-3321607	1138191130
3-rank ≥ 4	-653329427	-653329427	6454019
3-rank ≥ 5	-5393946914743	-5393946914743	6968
5-rank ≥ 2	-11199	-11199	1318152618
5-rank ≥ 3	-11203620	-11203620	13291706
5-rank ≥ 4	-258559351511807*	-1264381632596	4518
7-rank ≥ 2	-63499	-149519	296341915
7-rank ≥ 3	-501510767	-16974157711	1012251
7-rank ≥ 4		-469874684955252968120	67
11-rank ≥ 2	-65591	-126407	10333664
11-rank ≥ 3	-3035884424	-3532321517865683	8526
13-rank ≥ 2	-228679	-4060728916	2521258
13-rank ≥ 3	-38630907167	-2563347680683034101074499871	1243

Overall, the most notable entries are the 67 discriminants defining fields with 7-rank at least 4. To the best of our knowledge, these are the first fields found with this 7-rank. Additionally, the minimal discriminant $\Delta = -126438163259$ that we found is the smallest known example of a discriminant of a field with 5-rank 4. It is important to note that 3 fields with a 3-rank equal to 6 were found in [**23**]. Although this rank was not matched by our computations, a vast number of new 3-part structures were found. Arguably the most interesting among these are the two fields whose class groups have 3-part $C(3^9) \times C(3) \times C(3) \times C(3) \times C(3)$. Further data on exotic p-Sylow subgroups can be found in Tables A.1–A.5 in the Appendix.

Although a few examples of fields with 7-rank 3 were found in [**29**] and [**19**], and a few examples of fields of 11-rank 3 were found in [**15**], all the previous minimal discriminants for $p = 7$, 11 and 13 were found through our class computations described in [**20**]. This attests to the difficulty of developing effective techniques for constructing quadratic fields of high p-rank for larger primes p.

6. Conclusion

The numerical results show that our efforts to generalize and improve Diaz y Diaz's method for finding imaginary quadratic fields with 3-rank at least 2 have been successful in that they rapidly produce many fields with p-rank at least 2 with reasonably small discriminants. It is probable that the speed could be improved even more by implementing the algorithms in a lower-level language such as C/C++ as opposed to a high-level interpreted language like Sage. This would especially improve the efficiency of the sieving method for factoring described in Algorithm 3.1, as sieving benefits greatly from access to lower-level memory manipulation functionality.

The biggest obstacle to extending our search is the cost of class group computation. An obvious consideration would be to simply explore more efficient implementations for computing class groups. After testing a handful of large discriminants we found that Magma's `ClassGroup` [**30**] performed very similarly to PARI/GP's `quadclassunit`, so we opted for PARI/GP due to it being open-source and easier to access. There may be other implementations that can improve upon these by a small factor; although these would still have the same asymptotic complexity.

A more intriguing possibility for improvement is to devise a means to filter discriminants and identify, perhaps heuristically, those fields that are likely to have p-rank exceeding 2 before computing their class groups. This is exactly the approach that Quer used in his work finding imaginary quadratic fields with 3-rank equal to 6. The approach, mentioned briefly in [**23**] and in more detail in [**24**], is to estimate the L-function of an associated elliptic curve and, appealing to the Birch and Swinnerton-Dyer Conjecture, filter based on the estimated rank of the elliptic curve. The fact that elliptic curves with high rank correspond to imaginary quadratic fields with high 3-rank implies that this strategy heuristically picks out fields for which the 3-rank is likely to be large. We are currently exploring ideas for a similar approach for $p > 3$ which, if successful, should allow us to expand the search much further and hopefully find more interesting examples of exotic class group structures.

It would also be of interest to compare our methods to those of Mestre [**18**], Schoof [**25**], Léprevost [**15**], and Gillibert and Levin [**11**] that exploit the connections to algebraic geometry directly. Extending these methods and ours to search for real quadratic fields with large p-rank is another interesting project. Both of these research directions are under current investigation.

Appendix A. Data on Specific p-group Structures Found

Tables A.1–A.5 break down the different structures of the non-cyclic p-Sylow subgroups of the fields whose class groups were computed. In the column "p-part", a tuple $(e_1, e_2, \ldots, e_k)$ refers to a group structure $C(p^{e_1}) \times C(p^{e_2}) \times \cdots \times C(p^{e_k})$ where $C(n)$ denotes the cyclic group of order n. In Table A.1, all previous discriminants marked with a * were found in [**24**]. In Table A.2, they were found in [**19**]. To the best of our knowledge, these are the only examples provided in prior literature.

3-part	Previous* Min Δ	Min Δ Found	# Δ Found
(9,1,1,1,1)		-4781652142938583	2
(7,1,1,1,1)		-119901455891268	12
(6,2,1,1,1)		-21790632078441743	1
(6,1,1,1,1)		-606158852322299	28
(5,2,1,1,1)		-1139287867275027	4
(5,1,1,1,1)	-5579945937284287*	-16259689667204	72
(4,2,1,1,1)		-1502261884415659	8
(4,1,1,1,1)	-658417328546819*	-27551810196712	202
(3,2,1,1,1)	-9535792005606052*	-191422314332263	43
(3,1,1,1,1)	-1635609136827227*	-9516914581379	676
(2,2,1,1,1)	-1849337998495619*	-95959313694239	73
(2,1,1,1,1)	-35102371403731*	-20947933269332	1956
(1,1,1,1,1)	-5393946914743	-5393946914743	3891
(12,1,1,1)		-1189356312906079	13
(11,2,1,1)		-10641554173287823	1
(11,1,1,1)		-80496682329383	58

(10,2,1,1)		-232066870660487	12
(10,1,1,1)		-27009533351831	210
(9,2,2,1)		-1360416634735367	2
(9,2,1,1)		-59370495709911	37
(9,1,1,1)		-2706427613479	831
(8,3,1,1)		-434531603748116	6
(8,2,1,1)		-23985773289067	119
(8,1,1,1)	-226138531999	-226138531999	2493
(7,3,1,1)		-4817582128879	11
(7,2,2,1)		-56036578472779	1
(7,2,1,1)		-1792545911411	396
(7,1,1,1)	-513092626699	-513092626699	7344
(6,4,1,1)		-740469530387903	1
(6,3,2,1)		-253376492551619	1
(6,3,1,1)		-4032841753327	46
(6,2,2,1)		-14652095044139	4
(6,2,1,1)		-3930322587832	1205
(6,1,1,1)	-76951070303	-76951070303	22119
(5,4,1,1)		-30165947874743	3
(5,3,2,1)		-7405250027331172	1
(5,3,1,1)		-1190552839847	123
(5,2,2,1)		-58724498929819	18
(5,2,1,1)	-473827747963	-473827747963	3562
(5,1,1,1)	-7993105123	-7993105123	66887
(4,4,1,1)		-33516852803283	12
(4,3,2,1)		-17108559215023	1
(4,3,1,1)		-1579140273620	379
(4,2,2,1)		-18659260771715	56
(4,2,1,1)	-128589208863	-128589208863	10569
(4,1,1,1)	-3146813128	-3146813128	198721
(3,3,2,1)		-95139809105028	7
(3,3,1,1)	-1074734433547	-1074734433547	945
(3,2,2,1)		-1495321091551	128
(3,2,1,1)	-34245189208	-34245189208	32214
(3,1,1,1)	-5288116947	-5288116947	598482
(2,2,2,1)		-4324341977848	296
(2,2,1,1)	-32543535351	-32543535351	72053
(2,1,1,1)	-3972542271	-3972542271	1799341
(1,1,1,1)	-653329427	-653329427	3635311
(15,1,1)		-7412784971602919	4
(14,1,1)		-1199445898709711	41
(13,2,1)		-1959152115575119	11
(13,1,1)		-57329915311679	477
(12,3,1)		-7783345889181383	3
(12,2,1)		-315196348878431	72
(12,1,1)	-126690112721206499*	-6908116009031	2833

(11,3,1)		-868976039657431	8
(11,2,1)		-43222693504559	424
(11,1,1)	-797107037711	-1175416234151	12080
(10,4,1)		-5111867434551467	2
(10,3,1)		-179809468172935	40
(10,2,2)		-240547603651519	1
(10,2,1)		-2514065281111	1800
(10,1,1)	-146114436719	-146114436719	43389
(9,4,1)		-627212963493203	4
(9,3,1)		-9275890698391	214
(9,2,2)		-96789353990963	15
(9,2,1)	-581116399159	-581116399159	6574
(9,1,1)	-12792023879	-12792023879	139014
(8,4,1)		-110609652344647	20
(8,3,1)	-124071345551	-124071345551	703
(8,2,2)		-2668360754663	52
(8,2,1)	-59714529551	-86507761799	20457
(8,1,1)	-5347129751	-5347129751	426505
(7,5,1)		-251555051620699	1
(7,4,1)		-16488161012495	76
(7,3,2)		-71467687560212	10
(7,3,1)	-338926563823	-338926563823	2201
(7,2,2)	-484468933679	-484468933679	191
(7,2,1)	-4163792239	-4163792239	62982
(7,1,1)	-461309711	-461309711	1285263
(6,5,1)		-667219375024612	11
(6,4,1)	-276331426207	-276331426207	236
(6,3,2)		-2447509863143	31
(6,3,1)	-27291040424	-27291040424	6948
(6,2,2)	-9483757583	-9483757583	616
(6,2,1)	-376424303	-376424303	190687
(6,1,1)	-124438679	-124438679	3862973
(5,5,1)		-3115620789695	28
(5,4,1)	-186447381556	-186447381556	780
(5,3,2)	-78852105815	-1619378573304	93
(5,3,1)	-2232519167	-2232519167	21234
(5,2,2)	-45248632247	-45248632247	1786
(5,2,1)	-413771887	-413771887	572471
(5,1,1)	-32852423	-32852423	11593161
(4,4,2)		-134714111090772	5
(4,4,1)	-26320580987	-26320580987	1734
(4,3,2)	-295863285976	-583203069268	255
(4,3,1)	-522302531	-522302531	63043
(4,2,2)	-9766538987	-9766538987	5361
(4,2,1)	-53209523	-53209523	1718077
(4,1,1)	-13275687	-13275687	34762130

(3,3,3)		-13274921249572	4
(3,3,2)	-20687610651	-130708347771	565
(3,3,1)	-559587163	-559587163	143101
(3,2,2)	-18741973496	-18741973496	16009
(3,2,1)	-57236692	-57236692	5154730
(3,1,1)	-5153431	-5153431	104281796
(2,2,2)	-364435991	-364435991	32868
(2,2,1)	-101375499	-101375499	11598214
(2,1,1)	-3321607	-3321607	312801191
(1,1,1)	-4447704	-4447704	649355525
(16,1)		-6180709870676039	8
(15,1)		-419350731274151	258
(14,2)		-1416506636537519	23
(14,1)		-58458005876399	2291
(13,3)		-1659668122287311	5
(13,2)		-81328110739151	266
(13,1)		-7173077767151	13867
(12,3)		-271053539736983	28
(12,2)		-9360659630111	1549
(12,1)	-512068796879	-709319343599	62177
(11,4)		-1372147936838871	3
(11,3)		-11942231289719	181
(11,2)	-677250946319	-682812704279	6952
(11,1)	-52623967679	-97618013951	227654
(10,4)		-20528606822687	19
(10,3)	-766483839959	-1455104718671	778
(10,2)	-65798421911	-142692318479	25140
(10,1)	-8795475911	-11024762591	743425
(9,5)		-3069611062600312	1
(9,4)		-4478460907199	85
(9,3)	-60543925679	-60543925679	2863
(9,2)	-11901791639	-20980261727	82881
(9,1)	-1106108639	-1106108639	2312018
(8,5)		-18401222970803	11
(8,4)	-225796561799	-1819146689119	284
(8,3)	-37703425007	-52110784391	9331
(8,2)	-1173834359	-1173834359	256522
(8,1)	-98311919	-98311919	7012912
(7,5)	-253237383431	-42609838884859	41
(7,4)	-47649110911	-61201223599	1038
(7,3)	-3541241903	-6562836479	28716
(7,2)	-167885231	-167885231	780815
(7,1)	-32681951	-37648463	21096688
(6,6)		-28277864999519	3
(6,5)	-133786229531	-759780713491	107
(6,4)	-7274282423	-15644731279	3132

(6,3)	-636617543	-1043281091	87112
(6,2)	-19180391	-19180391	2347194
(6,1)	-3582743	-3582743	63312111
(5,5)	-6743415071	-423637980855	253
(5,4)	-4301015239	-12544040891	9715
(5,3)	-152637311	-152637311	261599
(5,2)	-15042011	-15042011	7039473
(5,1)	-508847	-599927	189936506
(4,4)	-136071631	-136071631	21968
(4,3)	-41361815	-49386703	782100
(4,2)	-1332167	-1332167	21134173
(4,1)	-29399	-153247	569760770
(3,3)	-6207263	-6207263	1762030
(3,2)	-351751	-351751	63397044
(3,1)	-17399	-17399	1709318817
(2,2)	-134059	-134059	142631063
(2,1)	-3299	-3299	5127934647
(1,1)	-3896	-3896	11532781211

Table A.1: 3-part structures

5-part	Previous* Min Δ	Min Δ Found	# Δ Found
(6,1,1,1)		-29223692703960901844	3
(5,1,1,1)		-23115910878760939104487	2
(4,2,1,1)		-39747358488997861867135	2
(4,1,1,1)		-2064918363990920	45
(3,2,1,1)		-713870092543251083672	1
(3,1,1,1)	-347546457876142204847*	-41131207995112	157
(2,2,1,1)		-2184031325678101777304	7
(2,1,1,1)	-630912818628505329119*	-238350381462199	881
(1,1,1,1)	-258559351511807*	-1264381632596	3420
(10,2,1)		-196282504615780102426427	1
(10,1,1)		-719668888494180546644	3
(9,1,1)		-601170377876508571	35
(8,2,1)		-11871279752301453854056	2
(8,1,1)		-106101520102380728	152
(7,2,1)		-88195933163985991143	6
(7,1,1)		-2659523746691179	826
(6,2,1)		-213409811170526583	58
(6,1,1)	-349008665407	-24339061404303	4013
(5,2,1)		-2665221927068163908	204
(5,1,1)	-25384593659	-3229265987256	20133
(4,3,1)		-6092229602869683	8
(4,2,1)	-116279191211	-1337006161770292	948
(4,1,1)	-3511272455	-66876865492	100883
(3,3,1)		-562954585788148276	35
(3,2,1)	-29867315295	-10241065678255	4797
(3,1,1)	-145367147	-890032871	502153

(2,2,2)	-287442559199	-15277416532031012543	5
(2,2,1)	-6896149079	-25987659771	20299
(2,1,1)	-51213139	-51213139	2512349
(1,1,1)	-11203620	-11203620	10124797
(14,1)		-283676995425795804340247	1
(13,1)		-110155263811937746685419	3
(12,1)		-317201690376439042287	26
(11,2)		-33291171086505137344699	1
(11,1)		-2594595364223905823	111
(10,2)		-46003432873651660003	4
(10,1)		-90960234921563435	608
(9,2)		-8369135150361181239	26
(9,1)		-7084251892338788	3012
(8,4)		-970644487236804090392	1
(8,3)		-20315924592054543155963	1
(8,2)		-25707908413976747	111
(8,1)	-941197327199	-68451950941652	15247
(7,3)		-4256081362984796723	3
(7,2)		-2769444241850843	622
(7,1)	-48662190359	-3270227349799	78092
(6,3)		-625532870037127003	36
(6,2)	-75913193999	-1078462086857560	3095
(6,1)	-1614153239	-57368333887	388458
(5,3)	-213265691687	-2861689046682709695	122
(5,2)	-5180829911	-155081563523	15706
(5,1)	-88527911	-1879050223	1945948
(4,4)		-1467852793757614031079	2
(4,3)	-10036313687	-103425154875416	663
(4,2)	-290810159	-36014679763	78091
(4,1)	-5820119	-5820119	9724229
(3,3)	-1068156239	-4455150346735	2581
(3,2)	-52456111	-670409895	389687
(3,1)	-621599	-621599	48614191
(2,2)	-1390367	-24994327	1626490
(2,1)	-50783	-50783	243070212
(1,1)	-11199	-11199	1012195234

Table A.2: 5-part structures

7-part	Previous* Min Δ	Min Δ Found	# Δ Found
(3,1,1,1)		-664652160708627486250579106056	1
(2,1,1,1)		-1884247051609224813123120596	8
(1,1,1,1)		-469874684955252968120	58
(9,1,1)		-1174046771147427850869466988072	1
(7,1,1)		-28446119246040006170662550815	6
(6,1,1)		-1709722545947903362406383	45
(5,1,1)		-44221073445452514723	416
(4,2,1)		-5438832486874599358067624	9
(4,1,1)	-356820088964	-429069139515571	2899
(3,3,1)		-211034216341933901480376896440	1

(3,2,1)		-2978654744508703	89
(3,1,1)	-19379510159	-27055504465317940	20359
(2,2,1)	-439240920004	-18841640731453242055	393
(2,1,1)	-648153647	-16974157711	140292
(1,1,1)	-501510767	-59220867124	847741
(11,1)		-31214462172510763995245455064	1
(10,1)		-362275360982619993364171755	10
(9,2)		-8603822104544671948771409471	1
(9,1)		-35194533384565143944891	45
(8,2)		-41829635402356017308666856635	1
(8,1)		-3485307074457345815895	355
(7,2)		-495829917565772785395811252	8
(7,1)		-65038453278281599	2376
(6,2)		-8884871244454699931797348	47
(6,1)	-174018745031	-137311936815726372	16983
(5,3)		-63799761056182467041071901543	1
(5,2)	-336699684383	-67208196536937832292	341
(5,1)	-5800676279	-1767950776916	118697
(4,3)		-1833032352201402190610115827	4
(4,2)	-16336216607	-835973339811751208	2330
(4,1)	-172820591	-66636642507	828102
(3,3)	-40111506371	-10848805860774663710437508	42
(3,2)	-528784319	-20261380249163	17068
(3,1)	-4603007	-115427951	5804875
(2,2)	-59288543	-11368726430052	103844
(2,1)	-480059	-3963944	40633451
(1,1)	-63499	-149519	248813333

Table A.3: 7-part structures

TABLE A.4. 11-part structures

11-part	Previous* Min Δ	Min Δ Found	# Δ Found
(5,1,1)		-482933822333784474655653100292965667	1
(4,1,1)		-241783869822537801905159591587	10
(3,1,1)		-1056523328545691539122184797287	78
(2,1,1)	-145931588651	-103121510852479373211114483	776
(1,1,1)	-3035884424	-3532321517864683	7661
(7,1)		-161246983809593497938056210142160841924	5
(6,1)		-8122060022255594570849043012	67
(5,1)	-935094698711	-1501588177054837992580	693
(4,2)		-42177966913676462762644	7
(4,1)	-7219509359	-139318644407667431	7690
(3,2)	-91355041631	-59268487604121704397283720	53
(3,1)	-218130623	-9955922266504	84028
(2,2)	-4536377039	-440953217421746725439861684	647
(2,1)	-7948999	-185328519	925340
(1,1)	-65591	-126407	9315134

Table A.5. 13-part structures

13-part	Previous* Min Δ	Min Δ Found	# Δ Found
(4,1,1)		-87316676344488903524279655272175378685698683	1
(3,1,1)		-26265546266831052453902561606133576	7
(2,1,1)	-105479207735	-61135051463420753760463404996	90
(1,1,1)	-38630907167	-256334768068303410107449987	1145
(7,1)		-22699509446220122346230885149354335802405399	1
(6,1)		-2963202904487970204245304707253023539	6
(5,1)		-8161147001077266804922786243	89
(4,1)	-55385334839	-76285684167795951751982711	1138
(3,2)	-366445322799	-4762935306033350578180863390302834359	12
(3,1)	-781846103	-43422255887258040	14787
(2,2)	-10692322055	-310637201042047641950817066472	85
(2,1)	-14127343	-50909788816791	191938
(1,1)	-228679	-4060728916	2313202

References

[1] C. Bagshaw, N. Rollick, M. J. Jacobson Jr., and R. Scheidler, *Code for improved methods for finding imaginary quadratic fields with high n-rank*, 2023. `https://github.com/ChristianBagshaw/Improved-methods-for-finding-imaginary-quadratic-fields-with-high-n-rank`.

[2] Karim Belabas, *On quadratic fields with large 3-rank*, Math. Comp. **73** (2004), no. 248, 2061–2074, DOI 10.1090/S0025-5718-04-01632-1. MR2059751

[3] Duncan A. Buell, *Class groups of quadratic fields*, Math. Comp. **30** (1976), no. 135, 610–623, DOI 10.2307/2005330. MR404205

[4] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62, DOI 10.1007/BFb0099440. MR756082

[5] Maurice Craig, *A type of class group for imaginary quadratic fields*, Acta Arith. **22** (1973), 449–459. (errata insert), DOI 10.4064/aa-22-4-449-459. MR318098

[6] Maurice Craig, *A construction for irregular discriminants*, Osaka Math. J. **14** (1977), no. 2, 365–402. MR450226

[7] Francisco Diaz y Diaz, *Sur les corps quadratiques imaginaires dont le* 3*-rang du groupe des classes est supérieur à* 1 (French), Séminaire Delange-Pisot-Poitou (15ème année: 1973/74), Théorie des nombres, Fasc. 2, Secrétariat Math., Paris, 1975, pp. Exp. No. G15, 10. MR392909

[8] F. Diaz y Diaz, *On some families of imaginary quadratic fields*, Math. Comp. **32** (1978), no. 142, 637–650, DOI 10.2307/2006174. MR485775

[9] F. Diaz y Diaz, Daniel Shanks, and H. C. Williams, *Quadratic fields with* 3*-rank equal to* 4, Math. Comp. **33** (1979), no. 146, 836–840, DOI 10.2307/2006320. MR521299

[10] N. Elkies, *post to NMBRTHRY mailing list*, 2016.

[11] Jean Gillibert and Aaron Levin, *A geometric approach to large class groups: a survey*, Class groups of number fields and related topics, Springer, Singapore, [2020] ©2020, pp. 1–15, DOI 10.1007/978-981-15-1514-9_1. MR4292539

[12] Michael J. Jacobson Jr. and Hugh C. Williams, *Solving the Pell equation*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, Springer, New York, 2009. MR2466979

[13] Helmut Koch, *Über den p-Klassenkörperturm eines imaginär-quadratischen Zahlkörpers* (German), Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, Bordeaux, 1974), Astérisque, No. 24-25, Soc. Math. France, Paris, 1975, pp. 57–67. MR392928

[14] Sige-Nobu Kuroda, *On the class number of imaginary quadratic number fields*, Proc. Japan Acad. **40** (1964), 365–367. MR170882

[15] Franck Leprévost, *Courbes modulaires et* 11*-rang de corps quadratiques* (French, with English and French summaries), Experiment. Math. **2** (1993), no. 2, 137–146. MR1259427

[16] Pascual Llorente and Jordi Quer, *On the* 3*-Sylow subgroup of the class group of quadratic fields*, Math. Comp. **50** (1988), no. 181, 321–333, DOI 10.2307/2007934. MR917838

[17] Cameron McLeman, *p-tower groups over quadratic imaginary number fields* (English, with English and French summaries), Ann. Sci. Math. Québec **32** (2008), no. 2, 199–209. MR2562045

[18] Jean-François Mestre, *Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques* (French), J. Reine Angew. Math. **343** (1983), 23–35, DOI 10.1515/crll.1983.343.23. MR705875

[19] N. Miller, *The structure of the class group if imaginary quadratic fields*, Master's thesis, Virginia Polytechnic Institute and State University, 2005.

[20] A. S. Mosunov and M. J. Jacobson Jr., *Unconditional class group tabulation of imaginary quadratic fields to $|\Delta| < 2^{40}$*, Math. Comp. **85** (2016), no. 300, 1983–2009, DOI 10.1090/mcom3050. MR3471116

[21] Trygve Nagel, *Über die Klassenzahl imaginär-quadratischer Zahlkörper* (German), Abh. Math. Sem. Univ. Hamburg **1** (1922), no. 1, 140–150, DOI 10.1007/BF02940586. MR3069394

[22] Carol Neild and Daniel Shanks, *On the 3-rank of quadratic fields and the Euler product*, Math. Comp. **28** (1974), 279–291, DOI 10.2307/2005835. MR352042

[23] Jordi Quer, *Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12* (French, with English summary), C. R. Acad. Sci. Paris Sér. I Math. **305** (1987), no. 6, 215–218. MR907945

[24] Jordi Quer Bosor, *Sobre el 3-rang dels cossos quadratics i la corba el.liptica Y('2) = X('3) + M*, ProQuest LLC, Ann Arbor, MI, 1987. Thesis (xx)–Universitat Autonoma de Barcelona (Spain). MR2714379

[25] R. J. Schoof, *Class groups of complex quadratic fields*, Math. Comp. **41** (1983), no. 163, 295–302, DOI 10.2307/2007782. MR701640

[26] Daniel Shanks, *New types of quadratic fields having three invariants divisible by 3*, J. Number Theory **4** (1972), 537–556, DOI 10.1016/0022-314X(72)90027-3. MR313220

[27] Daniel Shanks and Richard Serafin, *Quadratic fields with four invariants divisible by 3*, Math. Comp. **27** (1973), 183–187, DOI 10.2307/2005260. MR330097

[28] Daniel Shanks and Peter Weinberger, *A quadratic field of prime discriminant requiring three generators for its class group, and related theory*, Acta Arith. **21** (1972), 71–87, DOI 10.4064/aa-21-1-71-87. MR309899

[29] James J. Solderitsch, *Quadratic fields with special class groups*, Math. Comp. **59** (1992), no. 200, 633–638, DOI 10.2307/2153080. MR1139091

[30] The Computational Algebra Group, University of Sydney, *Magma*, 2023. available from `https://magma.maths.usyd.edu.au/magma/handbook/`.

[31] The PARI Group, Univ. Bordeaux, *PARI/GP version* `2.11.1`, 2018. available from `https://pari.math.u-bordeaux.fr/pub/pari/manuals/2.11.1/users.pdf`.

[32] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 8.8)*, 2017. `https://www.sagemath.org`.

[33] Yoshihiko Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka Math. J. **7** (1970), 57–76. MR266898

School of Mathematics and Statistics, University of New South Wales. Sydney, Australia

Email address: `c.bagshaw@unsw.edu.au`

Department of Computer Science, University of Calgary. Calgary, Canada

Email address: `jacobs@ucalgary.ca`

Department of Mathematics and Statistics and Department of Computer Science, University of Calgary. Calgary, Canada

Email address: `rscheidl@ucalgary.ca`

Centre for Education in Mathematics and Computing, University of Waterloo, Waterloo, Canada

Email address: `nrollick@uwaterloo.ca`