Imaginary quadratic number fields with class groups of small exponent

by

ANDREAS-STEPHAN ELSENHANS (Würzburg),
JÜRGEN KLÜNERS (Paderborn) and
FLORIN NICOLAE (București)

1. Introduction. Let $D$ be a fundamental discriminant, i.e. the discriminant of a quadratic number field. For $D < 0$ let $E(D)$ be the exponent of the ideal class group $\text{Cl}(D)$ of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$. Under the Extended Riemann Hypothesis it is known (see [BK], [W]) that $E(D) \gg \frac{\log |D|}{\log \log |D|}$. Without any unproved hypothesis it is not even known that $E(D) \to \infty$. In [W, Theorem 1] it is shown that there is at most one imaginary quadratic field with $|D| > 5460$ and $E(D) = 2$. In [BK], [W] it is shown (ineffectively) that there are finitely many imaginary quadratic fields with $E(D) = 3$. In [HB] Theorem 2] it is observed that for given $r \geq 0$ there are finitely many imaginary quadratic fields with $E(D) = 2^r$ or $E(D) = 3 \cdot 2^r$. (See also [EK].) Finally, there are finitely many imaginary quadratic fields with $E(D) = 5$ ([HB, Theorem 1]).

In this note we are interested in determining all $D$ such that the class group has exponent at most 8, i.e. $\text{Cl}(D)^c$ is the trivial group for some $c \leq 8$. In other words, we want the class group to be of type $C_2^r \times C_3^s, C_5^t, C_7^u$, or $C_2^r \times C_4^s \times C_8^t$, where $C_i$ denotes the cyclic group of order $i$. For any given $r, s$ it is known that there are infinitely many $D < 0$ such that $C_2^r \times C_4^s$ is a subgroup of $\text{Cl}(D)$.

Our computations show the following:

THEOREM 1. There are exactly 1555 imaginary quadratic fields with discriminant $|D| \leq 3.1 \cdot 10^{20}$ and class group of exponent $\leq 8$. The discriminants with more than seven decimal places are $-11148180, -12517428, -15337315, -15898740, -17168515, -28663635, -29493555, -31078723, -430950520.$

2010 Mathematics Subject Classification: Primary 11R29; Secondary 11R11.

Key words and phrases: class groups, imaginary quadratic fields.

Received 20 February 2018; revised 7 December 2018.

Published online 24 January 2020.

DOI: 10.4064/aa180220-20-3 [1] © Instytut Matematyczny PAN, 2020
Table 1. Number of imaginary quadratic fields with small exponent

| Exponent | Number of fields found | Field with largest discriminant |
|----------|------------------------|---------------------------------|
| 1        | 9                      | $\mathbb{Q}(\sqrt{-163})$      |
| 2        | 56                     | $\mathbb{Q}(\sqrt{-5460})$     |
| 3        | 17                     | $\mathbb{Q}(\sqrt{-4027})$     |
| 4        | 203                    | $\mathbb{Q}(\sqrt{-435435})$   |
| 5        | 27                     | $\mathbb{Q}(\sqrt{-37363})$    |
| 6        | 432                    | $\mathbb{Q}(\sqrt{-3761140})$  |
| 7        | 33                     | $\mathbb{Q}(\sqrt{-118843})$   |
| 8        | 778                    | $\mathbb{Q}(\sqrt{-430950520})$|

Since the database $[BM]$ contains the class groups of all imaginary quadratic number fields up to absolute discriminant $10^7$, we have only listed the larger fields in the preceding theorem. As already mentioned at the beginning of the introduction, it is (unconditionally) known that for exponent $2 \leq c \leq 8$, $c \neq 7$, there are only finitely many imaginary fields with exponent $c$. Unfortunately, these results are not effective. Therefore no complete explicit lists are known without using unproven conjectures.

**Theorem 2.** Assuming ERH, our computations found all fields for exponent up to 5 and 8. Assuming the non-existence of Siegel zeros, our computation found all fields with exponents 2, 4, 8.

Without assuming any unproven statement we can conclude that there is at most one missing field with exponent 2, 4 or 8.

Let $2 = p_1 < p_2 < \cdots$ be the sequence of prime numbers. For $n \geq 1$ let

$$d_n := p_1 \cdots p_n.$$  

In Section 4 we determine for given $r \geq 1$ a number $N_{2r}$ such that there is at most one imaginary quadratic field with $|D| \geq d_{N_{2r}}$ and $E(D) = 2^r$. For this we modify Weinberger’s technique from [W, Theorem 1]. For $r = 1$ we have $N_2 = 11$ and $d_{N_2} \leq 2.01 \cdot 10^{11}$. For $r = 2$ we have $N_4 = 24$ and $d_{N_4} \leq 2.38 \cdot 10^{34}$. For $r = 3$ we have $N_8 = 58$ and $d_{N_8} \leq 3.17 \cdot 10^{110}$. For $r = 4$ we have $N_{16} = 160$ and $d_{N_{16}} \leq 2.44 \cdot 10^{391}$.

In Section 5 we use lower class group bounds in order to compute all imaginary quadratic number fields with exponent 4 and 8, respectively. These bounds depend on the non-existence of Siegel zeros. If we do not want to assume any unproven conjecture we might miss at most one field. The main new idea in this approach is that we use upper bounds for the 4-rank of the class group by using the theory of Rédei matrices. Here it is helpful that on average we expect that the 4-rank is close to 1. This reduces dramatically the number of discriminants to consider.

In Section 6 we use Lemma 19 to effectively list all fields of exponent $c \leq 8$ which have smallest splitting prime $p \leq 197$. This already yields all
In a second step we use sieving techniques to find the fields of small exponent and discriminant $|D| < 3 \cdot 10^{23}$ which have smallest splitting prime greater than 197. For the implementation we use multiply-focused enumeration similar to [WW]. To the best of our knowledge these computations have been done for the first time.

The computed tables of fields and some programs can be found on the web page https://math.uni-paderborn.de/en/ag/ca/research/exponent/.

2. Some theoretical estimates. As before, let $D < 0$ be a fundamental discriminant. In the following we want to use the knowledge of a small split prime $p$, i.e. a prime $p \nmid D$ such that $pO_K = p \cdot \bar{p}$ splits in two different prime ideals in $K$. We are interested in a lower bound on the order of the ideal $p$ in the class group $\text{Cl}(D)$. The following lemma appears in different forms at least in [D, pp. 174–175], [BK, Lemma 2], [W, Lemma 5].

**Lemma 3.** Let $c > 0$ be an integer, let $p$ be a split prime in $K$, and let $p$ be a prime divisor of $p$ in $K$. If $p^c < |D|/4$, then the order of $p$ in the class group $\text{Cl}(D)$ is strictly larger than $c$.

As shown in Lemma 3 a small split prime in an imaginary quadratic number field already gives a good lower bound for the exponent of the class group. Here we want to use the extended Riemann hypothesis (ERH). Using this, we can prove:

**Theorem 4.** Let $K$ be a quadratic number field such that the absolute value of the discriminant $D$ is larger than $e^{25} \approx 7.2 \cdot 10^{10}$. Assume the extended Riemann hypothesis. Then there exists a split prime $p$ such that

$$p \leq (1.881 \log |D| + 2 \cdot 0.34 + 5.5)^2.$$

**Proof.** This is the result of Table 3 in [BS, p. 1731].

We remark that the paper [BS] gives similar statements with weaker constants for small discriminants. We used those in the following table for exponents smaller than or equal to 8.

| Exponent | Bound for $|D|$ |
|----------|---------------|
| 1        | $1.7 \cdot 10^7$ |
| 2        | $6 \cdot 10^6$ |
| 3        | $9.7 \cdot 10^{10}$ |
| 4        | $3.4 \cdot 10^{15}$ |
| 5        | $2.3 \cdot 10^{20}$ |
| 6        | $2.5 \cdot 10^{25}$ |
| 7        | $3.9 \cdot 10^{30}$ |
| 8        | $8.9 \cdot 10^{35}$ |
3. Using Siegel–Tatuzawa bounds. In the already cited paper, Weinberger suggested using efficient bounds based on Siegel zeros. Compared to the original Siegel bounds they have the advantage that the constants can be explicitly computed. Weinberger used this approach to determine (assuming that there are no Siegel zeros) all imaginary quadratic number fields of exponent 2. If one does not assume any unproven conjecture, it is shown that at most one field is missing.

For a fundamental discriminant $D$, using the Kronecker symbol we define the character

$$
\chi(n) := \chi_D(n) := \left( \frac{D}{n} \right).
$$

We associate to it the $L$-series

$$
L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \Re(s) > 0.
$$

Let $h(D) := |\text{Cl}(D)|$ be the class number of the field $K = \mathbb{Q}(\sqrt{D})$. For $D < -4$ it is well known that

$$
h(D) = \sqrt{|D|} L(1, \chi) / \pi.
$$

We are interested in good lower bounds for $L(1, \chi)$. It is known that there are no zeros of $L(s, \chi)$ for $\Re(s) \geq 1$. We get efficient lower bounds if we assume that no real zeros of $L(s, \chi)$ are close to 1. Tatuzawa Lemma 9 and Theorem 2 proved

**Lemma 5.** Let $0 < \varepsilon < 1/2$. There is at most one $|D| \geq \max(e^{1/\varepsilon}, e^{11.2})$ such that

$$
L(1, \chi) \leq \frac{0.655\varepsilon}{|D|^\varepsilon}.
$$

In this case $L(s, \chi)$ has a real zero $s$ with $1 - \varepsilon/4 < s < 1$.

As consequences we obtain

**Lemma 6.** Let $|D| > e^{11.2}$. If $L(s, \chi) \neq 0$ for $1 - \frac{1}{4\log|D|} \leq s < 1$ then

$$
h(D) > \frac{0.655}{\pi \varepsilon} \cdot \sqrt{|D|}.
$$

**Proof.** We apply Lemma 5 with $\varepsilon = 1/\log|D|$ to obtain

$$
L(1, \chi) > \frac{0.655\varepsilon}{|D|^\varepsilon} = \frac{0.655}{e \log|D|}.
$$

The class number formula $L(1, \chi) = \pi h(D)/\sqrt{|D|}$ yields the assertion. ■

**Lemma 7.** Let $A \geq e^{11.2}$. For all $|D| \geq A$ with at most one exception,

$$
h(D) > \frac{0.655}{\pi \log A} \cdot |D|^{1/2-1/\log A}.
$$
For $|D| = A^m$ with $m \geq 1$ we get
\[ h(D) > \frac{m \cdot 0.655 \sqrt{|D|}}{\pi e^m \log |D|} \]
with at most one exception.

Proof. We apply Lemma 5 with $\varepsilon = 1/\log A$ to obtain
\[ L(1, \chi) > \frac{0.655 \varepsilon}{|D|^\varepsilon}, \quad h(D) = \frac{\sqrt{|D|} L(1, \chi)}{\pi} > \frac{0.655}{\pi \log A} \cdot |D|^{1/2 - 1/\log A}, \]
for all $|D| \geq A$ with at most one exception. The second statement is a straightforward computation. \[ \square \]

The following lemma gives some improvement for the case with one exception.

Lemma 8. Let $A \geq 10^6$, $\varepsilon := 1/\log A$ and $m := \frac{\log |D|}{\log A}$. Then for all $D$ with $|D| \geq A$ we have, with at most one exception,
\[ L(1, \chi) \geq \min \left( \frac{1}{7.732 \log |D|}, 1.5 \cdot 10^6 \frac{\varepsilon}{|D|^\varepsilon} \right) \]
and
\[ (1) \quad h(D) \geq \min \left( \frac{\sqrt{|D|}}{\pi \cdot 7.732 \log |D|}, \frac{m \cdot 1.5 \cdot 10^6 \sqrt{|D|}}{\pi e^m \log |D|} \right). \]
Note that for $m \leq 19.2$ the first number is the minimum.

Proof. This is the main result of \[ C \]. \[ \square \]

Let us compare the result of Lemma 8 with Lemmata 6 and 7. When comparing Lemma 6 with Lemma 8, we see that Lemma 6 gives a lower class group bound which is about a factor of 2 better. But here we have to assume that there are no Siegel zeros. When we compare Lemma 7 with Lemma 8, we see that for $m \geq 2.6$ Lemma 8 is better. Note that the second number in the minimum is always better than the bound in Lemma 7. Furthermore it is important to note that $(10^6)^{19.2} > 10^{115}$, which is sufficient for all our computations for exponent 8.

4. Fields with exponent a power of two. Weinberger \[ W \] Theorem 1 proved that there is at most one imaginary quadratic field with $|D| > 5460$ and $E(D) = 2$. To extend his result to exponent $2^r$, we modify his technique. Let $2 = p_1 < p_2 < p_3 < \cdots$ be the sequence of prime numbers. For $n \geq 1$ let
\[ d_n := p_1 \cdot \ldots \cdot p_n. \]
In this section we determine for given $r \geq 1$ a number $N_{2^r}$ such that there is at most one imaginary quadratic field with $|D| \geq d_{N_{2^r}}$ and $E(D) = 2^r$. 
Lemma 9. Let \( D < 0 \) be a fundamental discriminant. If \( E(D) = 2^r \) with \( r \geq 1 \) then
\[
h(D) \leq 2^{r(\omega(D) - 1)}.
\]

Proof. If \( E(D) = 2^r \) then \( \text{Cl}(D) \) is isomorphic to \( C_2^{a_1} \times C_2^{a_2} \times \cdots \times C_2^{a_r} \), \( a_1 \geq 0, \ldots, a_{r-1} \geq 0, a_r > 0 \), and we have
\[
h(D) = 2^{a_1 + 2a_2 + \cdots + ra_r}.
\]
By genus theory, \( a_1 + \cdots + a_r = \omega(D) - 1 \), hence
\[
h(D) = 2^{a_1 + 2a_2 + \cdots + ra_r} \leq 2^{r(a_1 + \cdots + a_r)} = 2^{r(\omega(D) - 1)}.
\]

Lemma 10. If \( D \) is a fundamental discriminant then
\[
|D| \geq d_{\omega(D)}.
\]

Proof. We have
\[
D = \prod_{p \mid |D|} p^*\]
with \( 2^* \in \{-4, -8, 8\} \) and \( p^* = (-1)^{(p-1)/2}p \) for \( p \neq 2 \), hence
\[
|D| \geq p_1 \cdots p_{\omega(D)} = d_{\omega(D)}.
\]

Theorem 11. Let \( r \geq 1 \) be an integer. Let \( N_{2r} \) be the smallest integer \( N \) such that
\[
d_N \geq e^{11.2}, \quad p_N^{1/2 - 1/\log d_N} \geq 2^r, \quad \frac{0.655}{\pi e} \cdot \sqrt{\frac{d_N}{\log d_N}} \geq 2^{r(N-1)}.
\]
Let \( D < 0 \) be a fundamental discriminant with \( |D| \geq d_{N_{2r}} \). If \( L(s, \chi) \neq 0 \) for \( 1 - \frac{1}{4\log |D|} \leq s < 1 \) then \( E(D) \neq 2^r \).

Without any assumption on zeros of \( L \)-functions, there is at most one \( D \) with \( |D| \geq d_{N_{2r}} \) and \( E(D) = 2^r \).

Proof. Let \( N \geq 1 \) be an integer as in the hypothesis. Assume that \( L(s, \chi) \neq 0 \) for \( 1 - \frac{1}{4\log |D|} \leq s < 1 \). We apply Lemma 6 to obtain
\[
h(D) > \frac{0.655}{\pi e} \cdot \frac{\sqrt{|D|}}{\log |D|}.
\]
Suppose that \( E(D) = 2^r \). Lemma 9 implies
\[
2^{r(\omega(D) - 1)} > \frac{0.655}{\pi e} \cdot \frac{\sqrt{|D|}}{\log |D|} \geq \frac{0.655}{\pi e} \cdot \frac{\sqrt{d_N}}{\log d_N} \geq 2^{r(N-1)},
\]
hence \( \omega(D) > N \). By Lemma 10 we have
\[
|D| \geq d_{\omega(D)} \geq d_N \cdot p_N^{\omega(D) - N},
\]
Let \( D \) be a discriminant such that \( \omega(D) > N \). By Lemma 9 and the choice of \( N \) we have

\[
2^{r(\omega(D)-1)} > h(D) > \frac{0.655}{\pi \log d_N} \cdot |D|^{1/2-1/\log d_N} \geq 2^{r(N-1)},
\]

hence \( \omega(D) > N \). By Lemma 10, \(|D| \geq d_{\omega(D)} > d_N \cdot p_N^{\omega(D)-N} \), so

\[
2^{r(\omega(D)-1)} \geq h(D) > \frac{0.655}{\pi \log d_N} \cdot |D|^{1/2-1/\log d_N}
\]

\[
> \frac{0.655}{\pi \log d_N} \cdot d_N^{1/2-1/\log d_N} \cdot p_N^{(\omega(D)-N)(1/2-1/\log d_N)}
\]

\[
= \frac{0.655}{\pi} \cdot \frac{d_N^{1/2-1/\log d_N}}{\log d_N} \cdot 2^{r(\omega(D)-N)} \cdot \left( \frac{p_N^{\omega(D)-N}}{2^r} \right)^{\omega(D)-N}
\]

\[
\geq \frac{0.655}{\pi} \cdot \frac{d_N^{1/2-1/\log d_N}}{\log d_N} \cdot 2^{r(\omega(D)-N)},
\]
since \((p_N^{1/2 - 1/\log d_N}/2^r)^\omega(D) - N \geq 1\) by the hypothesis \(p_N^{1/2 - 1/\log d_N} \geq 2^r\). It follows that
\[
2^r(N-1) > \frac{0.655}{\pi} \cdot \frac{d_N^{1/2 - 1/\log d_N}}{\log d_N} = \frac{0.655}{\pi e} \cdot \frac{\sqrt{d_N}}{\log d_N},
\]
in contradiction with the hypothesis
\[
\frac{0.655}{\pi e} \cdot \sqrt{d_N} \log d_N \geq 2^r(N-1).
\]
So \(E(D) \neq 2^r\). 

**Example.** For \(r = 1\) we have \(N_2 = 11\) and \(d_{N_2} \leq 2.01 \cdot 10^{11}\). For \(r = 2\) we have \(N_4 = 24\) and \(d_{N_4} \leq 2.38 \cdot 10^{34}\). For \(r = 3\) we have \(N_8 = 58\) and \(d_{N_8} \leq 3.17 \cdot 10^{110}\). For \(r = 4\) we have \(N_{16} = 160\) and \(d_{N_{16}} \leq 2.44 \cdot 10^{391}\).

### 5. Algorithm using Siegel bounds.
In this section we want to use the estimates from Lemmata 6 and 8 in order to compute all imaginary quadratic number fields with exponent 4 or 8. When we use the bounds from Lemma 6 we potentially miss fields such that the corresponding \(L\)-series has a Siegel zero close to 1. The estimate from Lemma 8 is a little weaker. This leads to more expensive computations, but it has the advantage that we can prove that we miss at most one field. These estimates are not valid for fields with small discriminant. This is not a big problem, since the class groups of fields with small discriminants are known. E.g. the web-page [BM](http://example.com) provides a table of all quadratic fields up to absolute discriminant \(10^7\). We checked the small fields independently by computations in Magma without using any unproven conjectures.

Let \(c \in \{4, 8\}\) be the exponent we are looking for. Then we split our problem by looking at discriminants with \(k\) different prime factors. The estimates in Section 4 show that we can bound the maximal number of prime factors. In the following we write our discriminants as products of \(k\) fundamental discriminants \(p^*\). For every odd prime \(p\) we have \(p^* = (-1)^{(p-1)/2p}\), and \(2^* \in \{-4, -8, 8\}\).

In the following let
\[
D = p_1^* \cdots p_k^*,
\]
where we assume that \(p_1 < \cdots < p_k\).

From genus theory it is well known that the 2-rank of \(\text{Cl}(D)\) is exactly \(k - 1\). When we assume that the class group is of exponent \(c\), the maximal possible class group is \((\mathbb{Z}/c\mathbb{Z})^{k-1}\) and therefore of order \(c^{k-1}\). Using the estimates of Lemma 6 or 8 we can compute an upper bound for the absolute value of \(D\). The basic idea of the algorithm is to test all \(D\) smaller than this bound consisting of exactly \(k\) prime factors. When \(k\) is large it is not practical to list and test all those \(D\). Therefore we would like to reduce this list further. The 4-rank of class groups of quadratic number fields is well studied and
there are nice formulas to compute it. Furthermore, it is known that the average 4-rank is small \[\text{[FK, G]}\]. Assume that we know the 4-rank \(r_4\) of \(\text{Cl}(D)\) and denote by \(r_2 := k - 1\) the 2-rank. Then the maximal possible class group of exponent \(c\) improves to

\[
\left(\mathbb{Z}/c\mathbb{Z}\right)^{r_4} \times \left(\mathbb{Z}/2\mathbb{Z}\right)^{r_2-r_4}
\]

of order \(2^{r_2-r_4}c^{r_4}\).

This gives an improvement by a factor of \((c/2)^{r_2-r_4}\).

5.1. Rédei matrices. In this section we study the 4-rank of the class group of quadratic number fields. The results used in this subsection are well known and based on the work of Rédei. In the following we use the Kronecker symbols \(\left(\frac{D}{p}\right)\) and corresponding to \(D = p_1^* \cdots p_k^*\) we define the matrix \(M = (c_{ij}) \in \mathbb{F}_2^k\) via

\[
(-1)^{c_{ij}} := \left(\frac{p_j^*}{p_i}\right) \quad \text{for} \quad 1 \leq j \neq i \leq k \quad \text{and} \quad c_{ii} := \sum_{j=1, j \neq i}^k c_{ij}, \quad 1 \leq i \leq k.
\]

**Theorem 12** (Rédei \[\text{[R, 10.b]}, \text{[G, (2.7)]}\]). Let \(D = p_1^* \cdots p_k^*\). Then \(\text{rk}_4(\text{Cl}(D)) = k - 1 - \text{Rank}(M)\).

The relation \(c_{ii} := \sum_{j=1, j \neq i}^k c_{ij}\) for \(1 \leq i \leq k\) shows that the last column of \(M\) is the sum of the first \(k - 1\) columns and therefore dependent on the first \(k - 1\) columns. Furthermore, by the multiplicativity of the Kronecker symbol,

\[
(-1)^{c_{ii}} = \left(\frac{\prod_{j=1, j \neq i}^k p_j^*}{p_i}\right).
\]

In order to understand this matrix, the following lemma is helpful. It also deals with the prime 2 except when \(2^* = -4\).

**Lemma 13.** Let \(p_i\) and \(p_j\) be different prime numbers such that \(p_i^* \neq -4 \neq p_j^*\). Then

\[
\left(\frac{p_i^*}{p_j}\right)\left(\frac{p_j^*}{p_i}\right) = \begin{cases} 1, & p_i^* > 0 \text{ or } p_j^* > 0, \\ -1, & p_i^* < 0 \text{ and } p_j^* < 0. \end{cases}
\]

The proof is straightforward from the reciprocity law. From this we see that if we have two different primes congruent to 3 modulo 4 dividing \(D\) then we get an entry 1 in our matrix. Furthermore the matrix is not symmetric.

In our algorithm we compute a lot of Rédei matrices and the corresponding ranks. In order to simplify these computations we check when the last row is the sum of the first \(k - 1\) rows.

**Lemma 14.** Let \(D = p_1^* \cdots p_k^* < 0\) be a product of fundamental discriminants with \(p_1 < \cdots < p_k\) and denote by \(M\) the Rédei matrix and by the vector \((d_1, \ldots, d_k)\) the sum of the rows of \(M\).
Assume that \( p_1^* \neq -4 \). Then the vector \((d_1, \ldots, d_k)\) is zero. In the case \( p_1^* = -4 \) we define \( D := -D/4 \) and we get

\[
((-1)^{d_1}, \ldots, (-1)^{d_k}) = \left( \left( \frac{2}{D} \right), \left( \frac{2}{p_2} \right), \ldots, \left( \frac{2}{p_k} \right) \right).
\]

**Proof.** The sum of the \( j \)th column is 0 if and only if the product of the corresponding symbols in the exponents are 1. We get for this product:

\[
\prod_{i=1, i \neq j}^{k} \left( \frac{p_i^*}{p_j} \right) \cdot \left( \prod_{i=1, i \neq j}^{k} \frac{p_i^*}{p_i} \right) = \prod_{i=1, i \neq j}^{k} \left( \frac{p_j^*}{p_i} \right) \left( \frac{p_i^*}{p_j} \right).
\]

If \( p_1^* \neq -4 \), we are able to apply Lemma 13. If \( p_j^* > 0 \) then all factors are 1. If \( p_j^* < 0 \) then the number of negative \( p_i^* \neq p_j^* \) is even and therefore the product is 1.

It remains to study the case \( p_1^* = -4 \). If we multiply the product (3) by \( \prod_{i=2}^{k} \left( \frac{2}{p_i} \right) \) if \( j = 1 \) and by \( \left( \frac{2}{p_j} \right) \) for \( j \neq 1 \) we get the product for \( 2^* = -8 \) and we know that this product is 1. Therefore the product is as expected. ■

Note that for \( p_1^* = -4 \) we only get row sum 0 if all odd prime divisors are congruent to \( \pm 1 \) mod 8.

Using Theorem 12 we know that \( \text{rk}_4(\text{Cl}(D)) = k - 1 - \text{Rank}(M) \). Therefore we are interested in good lower bounds for the rank of the Rédei matrix \( M \). Denote by \( t \) the number of negative \( p_i^* \). Then \( \text{Rank}(M) \geq (t - 1)/2 \) (see [S]). That paper also discusses the cases where this bound is sharp.

**5.2. Using the Rédei matrix.** In this section we describe an algorithm to compute all fields with exponent \( c = 2^r \), where we focus on the cases \( c = 4, 8 \). In order to use the Rédei matrices we restrict to discriminants with exactly \( k \) prime factors. Using Lemma 8 we can give an upper bound for the number of prime factors for fields of exponent \( 2^r \) which is valid for all fields with at most one exception. In the example after Theorem 11 we get 11, 24, 58 for exponents 2, 4, 8, respectively. We remark that these bounds can be improved, but the following algorithm is very efficient for the cases close to the bound. For a given exponent \( c = 2^r \) we call the following algorithm for all \( k \geq 1 \) up to the computed upper bound.

For the algorithm we have to decide whether we want to use the lower bound of Lemma 6 or of Lemma 8. The first lemma has the advantage that the bound is better and therefore the computation will be faster. In this case we only compute all the relevant fields which have no Siegel zero. If we assume that no Siegel zeros exist, then this computation is complete. The bound of the second lemma is weaker, but it has the advantage that we miss at most one field (if it exists, it has a Siegel zero). In our range for exponent 8, this bound is about a factor of 2 weaker than the first bound. In order to
simplify the presentation we only give the description of the algorithm using the bound of Lemma 8.

The main algorithm to call is Algorithm 18. This algorithm computes the global variables $B_0, \ldots, B_k$ to be used in Algorithms 15 and 17. The main idea of the algorithms is that the knowledge of a factor of $D$ gives some partial information on the Rédei matrix. This information can be used to give an upper bound on the 4-rank of the class group which then gives improved bounds on the maximal possible discriminant. In theory we expect that the average 4-rank is close to 1 [G] and therefore the upper bound $c^{k-1}$ for the class number of a field with exponent $c$ is quite pessimistic. The described approach improves the upper bound of the class number, and therefore the maximal possible discriminant, when the lower rank bound of the Rédei matrix increases, and therefore the possible 4-rank decreases.

The goal of the first algorithm is to give a quick check if the fundamental discriminant $D = p_1^* \cdots p_k^*$ has an exponent which is a divisor of $c$. The correctness of the algorithm is obvious on account of Lemma 3. If possible, we try to avoid the actual computation of the class group.

**Algorithm 15 (Check($c, p_1^*, \ldots, p_k^*$)).**

*Input:* Exponent $c = 2^r$, prime fundamental discriminants $p_1^*, \ldots, p_k^*$.  
*Output:* Return true iff $D = p_1^* \cdots p_k^* < 0$ and the exponent of the class group of $\mathbb{Q}(\sqrt{D})$ is a divisor of $c$.

*Step 1:* If $D := p_1^* \cdots p_k^* > 0$ then return false.

*Step 2:* Compute the smallest prime $q$ which is split in $K := \mathbb{Q}(\sqrt{D})$.

*Step 3:* If $q^c < |D|/4$ then return false (see Lemma 3).

*Step 4:* If the $c$th power of a prime ideal above $q$ is not principal, then return false. This test can be done most efficiently by using binary quadratic forms.

*Step 5:* Repeat the test of Step 4 with the 2nd smallest splitting prime.

*Step 6:* Compute the rank $s$ of the Rédei matrix of $D$. If $|D| > B_s$ then return false ($B_s$ is a global variable computed in Algorithm 18).

*Step 7:* Compute the class group of $K$. If the exponent divides $c$ then return true, otherwise return false.

Let $D = p_1^* \cdots p_k^*$ be a negative fundamental discriminant and assume that $p_1^*, \ldots, p_\ell^*$ are known to us. Let $M$ be the Rédei matrix of $D$ defined in Section 5.1. Denote by $N$ the minor defined by the first $\ell$ rows and first $\ell$ columns. Trivially, $\text{Rank}(N) \leq \text{Rank}(M)$. Since $p_1^*, \ldots, p_\ell^*$ are known to us, we can compute all entries of $N$ except the diagonal. The following algorithm tests all possible combinations for the diagonal and therefore computes a lower bound for the rank of $N$ and $M$.  

**Algorithm 16 (Check($c, p_1^*, \ldots, p_\ell^*$)).**

*Input:* Exponent $c = 2^r$, prime fundamental discriminants $p_1^*, \ldots, p_\ell^*$.  
*Output:* Return true iff $D = p_1^* \cdots p_\ell^* < 0$ and the exponent of the class group of $\mathbb{Q}(\sqrt{D})$ is a divisor of $c$.

*Step 1:* If $D := p_1^* \cdots p_\ell^* > 0$ then return false.

*Step 2:* Compute the smallest prime $q$ which is split in $K := \mathbb{Q}(\sqrt{D})$.

*Step 3:* If $q^c < |D|/4$ then return false (see Lemma 3).

*Step 4:* If the $c$th power of a prime ideal above $q$ is not principal, then return false. This test can be done most efficiently by using binary quadratic forms.

*Step 5:* Repeat the test of Step 4 with the 2nd smallest splitting prime.

*Step 6:* Compute the rank $s$ of the Rédei matrix of $D$. If $|D| > B_s$ then return false ($B_s$ is a global variable computed in Algorithm 18).

*Step 7:* Compute the class group of $K$. If the exponent divides $c$ then return true, otherwise return false.
**Algorithm 16 (LowerRédeiBound($p_1^*, \ldots, p_\ell^*$)).**

**Input:** Prime fundamental discriminants $p_1^*, \ldots, p_\ell^*$ with $\ell < k$.

**Output:** Return a lower bound for the rank of the Rédei matrix of all $D$ where $D$ has exactly $k$ prime factors and $p_1^* \cdots p_\ell^* | D$.

**Step 1:** For all $1 \leq i \neq j \leq \ell$ compute $c_{ij}$ via $(-1)^{c_{ij}} := \left(\frac{p_j}{p_i}\right)$.

**Step 2:** For all $(a_1, \ldots, a_\ell) \in \mathbb{F}_2^\ell$ compute the rank of the matrix $D = (d_{ij})$, where $d_{ij} = c_{ij}$ for $i \neq j$ and $d_{ii} = a_i$.

**Step 3:** Return the minimal rank computed in Step 2.

In the following algorithm we denote by $P[i]$ the $i$th prime number. We update the lower bound of the rank of the Rédei matrix and append the next fundamental prime discriminant. This function will call itself recursively. The number $m$ is the index of the smallest prime that can be used next.

**Algorithm 17 (NextTuple($m$, Discs, $k$, c)).**

**Input:** Number $m$ of the next prime to use, list Discs = $[p_1^*, \ldots, p_\ell^*]$ of fundamental prime discriminants, $k$, exponent $c = 2^r$.

**Output:** List of all discriminants $D$ with $k$ prime factors such that $p_1^* \cdots p_\ell^* | D$ (with at most one exception).

**Step 1:** $s := $ LowerRédeiBound($p_1^*, \ldots, p_\ell^*$).

**Step 2:** $B := B_s$, res:= $\{\}$ (empty list), bound := $B/(|p_1^* \cdots p_\ell^*|)$, $i := m$, $C := P[i] \cdots P[i + k - \ell - 1]$.

**Step 3:** While $C \leq$ bound do

1. $p_{\ell+1}^* := (-1)^{(P[i]-1)/2} P[i]$.
2. If $k = \ell + 1$ then call Check($c$, $p_1^*, \ldots, p_k^*$) and append $D = p_1^* \cdots p_k^*$ to res if the check is successful.
3. If $k > \ell + 1$ then call NextTuple($i$, $\{p_1^*, \ldots, p_{\ell+1}^*\}$, $k$, c) and append the computed $D$’s to res.

4. $i := i + 1$, $C := P[i] \cdots P[i + k - \ell - 1]$.

**Step 4:** Return res.

In the main algorithm we compute the global variables $B_0, \ldots, B_{k-1}$ and we split the computation into four parts, depending on the behavior at 2.

**Algorithm 18 (Computation of fields with exponent $2^r$).**

**Input:** Exponent $2^r$, number of prime factors $k$.

**Output:** All fields with exponent $c = 2^r$ with at most one exception.

**Step 1:** By numerical approximation compute a bound $B_\ell$ for all $0 \leq \ell \leq k-1$ such that for all $|D| > B_\ell$ the minimum of (1) is greater than $2^\ell \cdot c^{k-1-\ell}$.

**Step 2:** Call res1 := NextTuple(2, $\{\}$, $k$, c).

**Step 3:** Call res2 := NextTuple(2, $\{-4\}$, $k$, c).
Step 4: Call res3 := NextTuple(2, \{-8\}, k, c).
Step 5: Call res4 := NextTuple(2, \{8\}, k, c).
Step 6: Return the discriminants from res1, res2, res3, res4.

We remark that there are obvious improvements in the implementation which we have not described here for simplicity. For instance in the algorithm LowerRédeiBound we already know in Step 1 the \(c_{ij}\) for \(i, j < \ell\) with \(i \neq j\) from an earlier iteration. Note that there might be one missing example for the overall algorithm by using Lemma 8. The reason is that we compute all fields with exponent dividing \(c\) assuming the bounds of Lemma 8. Therefore missing examples have the property that the bounds of Lemma 8 are wrong and this can happen at most once.

The algorithm described above only computes discriminants \(D\) such that \(|D| > 10^6\). We could easily reduce this bound, but this is not an issue since there are known tables of class groups for all quadratic fields of small discriminant. The web-page [BM] gives all fields up to \(10^7\).

The overall running time of our algorithm on one core is about 17 hours when we use the estimates from Lemma 6. The cases \(k \in \{30, \ldots, 58\}\) take about 50 seconds. Only for small \(k\) do we need to compute class groups. The cases \(k \leq 6\) take about half an hour. The most expensive cases are \(k \in \{8, \ldots, 12\}\) which take more one hour each, the worst case being \(k = 10\) which takes almost three hours.

When we use the estimates from Lemma 8 which are sufficient to prove that we miss at most one example, the running time is about 60 hours. In case we can take a bound which is a factor of 2 better than the bound in Lemma 6 the running time improves to less than three hours.

We remark that the approach in this section can only be applied to exponents which are powers of 2. When we apply our program to exponent 2, we need less than ten seconds to compute all fields with \(|D| > 1000\). For exponent 4, the corresponding running time is about ten minutes. For exponent 9 our running time was about 60 hours. We tried to do exponent 16, but with the current methods this seems to be an impossible task.

6. Direct searching for small discriminants. When assuming ERH, the exponent of the class group and Theorem 4 lead to a bound on the discriminant. Now we have to test the finite number of discriminants up to this bound. Here, we present a two-stage approach for this. In the first stage we search for the fields that have fixed smallest split prime \(p \in \{2, \ldots, 197\}\). In the second stage we confirm by sieving that no such field with smallest split prime > 197 exists.

For efficiency all computations are adapted to the 64-bit arithmetic of modern-day computers. It turns out that the first stage can be done up
to exponent 8, and the sieving in the second stage can be done up to the ERH-based bound for exponent 5.

**Lemma 19.** For a prime $p$ and an exponent $c$ there are less than $2^{p^{c/2}}$ imaginary quadratic fields $K = \mathbb{Q}(\sqrt{D})$ such that $p$ splits in $K$ and the ideal above $p$ has order divisible by $c$ in the class group.

**Proof.** The assumption implies that the equation $4p^c = x^2 + |D|y^2$ has an integer solution with $x \cdot y \neq 0$. Thus, the field $K$ is one of $\mathbb{Q}(\sqrt{-4p^c - x^2})$ for $x \in \mathbb{Z}$ and $4p^c - x^2 > 0$. This shows $1 \leq x < 2^{p^{c/2}}$. Thus, there are less than $2^{p^{c/2}}$ fields. □

**Remarks 20.** 1. The lemma above results in an algorithm to enumerate all imaginary quadratic fields such that $p$ is a split prime and the exponent of the class group is a divisor of $c$. We have to test $O(p^{c/2})$ discriminants. More precisely, we first compute a finite list of fields that is a superset of the fields we are searching. The superfluous fields can easily be removed in a second step.

2. As a slight variation, we can enumerate all quadratic fields such that $p$ is the smallest split prime and the exponent of the class group divides $c$. For this we just have to sift out all those fields that have a smaller split prime. Note that this can be done without factoring $Dy^2 = 4p^c - x^2$.

3. A C-implementation of this approach lists all the fields with smallest split prime $\leq 197$ and $c = 8$ in less than four minutes. We find 268 fields with exponent 1,2,4 and 778 fields with exponent 8. The largest one is $\mathbb{Q}(\sqrt{-430950520})$.

4. Doing the same computation with exponents 3, 5, 6, 7 takes less than a minute.

5. An imaginary quadratic field with class group exponent $\leq 8$ not listed has smallest split prime $> 197$.

Now we have to search for the imaginary quadratic fields with $|D|$ up to a given bound and smallest split prime $> 197$. This can be done by a multiply-focused enumeration similar to [WW].

**Remarks 21.** To maximize the speed of the search for fields with no split prime $p \leq 197$ and $|D| < 3 \cdot 10^{20}$ we used bit-level operations and tables of pre-computed data. Further, non-negative integers $< 2^{64}$ have the fastest arithmetic. Thus, the main loop should be restricted to this.

This results in the following approach:

- We want to search for all imaginary quadratic fields $\mathbb{Q}(\sqrt{D})$ with smallest split prime $> 197$. This implies \( \left( \frac{D}{p} \right) \neq 1 \) for all primes $p \leq 197$.

- By the Chinese remainder theorem with the module \( m = 16 \cdot 3 \cdot 5 \cdots 47 \approx 4.9 \cdot 10^{18} \) the number of possible residue classes for $|D|$ is $220172127436800 \approx 2.2 \cdot 10^{14}$. 
• Let \( r \) be the smallest non-negative representative of a feasible residue class modulo \( m \). We have to test the fields with \(|D| = r, r + m, r + 2m, \ldots, r + 63m\) in parallel.

• The prime 53 rules out a field if \((\frac{D}{53}) = 1\). For \(|D| = r, r + m, r + 2m, \ldots, r + 63m\), we can encode this in a sequence of 64 bits. The \( k \)th bit is 1 iff the field for \(|D| = r + km\) is not ruled out by \((\frac{-r - km}{53}) = 1\).

We tabulate these bit sequences for each residue class of \( r \) mod 53.

• Similarly for each other prime \( p \leq 197 \) and each residue class \( r \) mod \( p \) we get a sequence of 64 bits. The \( k \)th bit is 1 iff the field for \(|D| = r + km\) is not ruled out by \((\frac{-r - km}{p}) = 1\).

This gives us further tables of bit sequences, one table for each prime \( p \) with one entry of 64 bits for each residue class of \( r \) mod \( p \).

• To combine the information modulo the various primes, we have to pick those \(|D|\) that are not ruled out by one of the primes up to 197. In the language of bit sequences this means that we have to do logical \textbf{and} of the sequences.

• If a result bit of the \textbf{and} is 0, the corresponding field is ruled out.

• If a result bit is 1, the field \( \mathbb{Q}(\sqrt{-r - km}) \) needs a more detailed inspection.

This approach leads to the following algorithm.

\begin{algorithm}
\textbf{Algorithm 22} (Multifocused bit-vector sieve).
\begin{itemize}
  \item \textbf{Input:} No input.
  \item \textbf{Output:} Print all imaginary quadratic fields \( \mathbb{Q}(\sqrt{D}) \) without smallest split prime \( p > 197 \), \(|D| < 3.1 \cdot 10^{20} \) and \( 4p^8 > |D| \).
  \item \textbf{Step 1:} Set \( m_1 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 = 255255 \), \( m_2 = 19 \cdot 23 \cdot 29 \cdot 31 = 392863 \), \( m_3 = 37 \cdot 41 \cdot 43 \cdot 47 = 3065857 \), and \( m = 16m_1m_2m_3 \approx 4.9 \cdot 10^{18} \).
  \item \textbf{Step 2:} For each module \( m_i \) compute a list of the integers \( r \) in \( \{0, \ldots, m_i - 1\} \) such that \((\frac{-r}{p}) \neq 1\) for all primes \( p \) dividing \( m_i \).
  \item \textbf{Step 3:} For each prime \( p \leq 197 \) not dividing \( m \) set up a list \((l_p[0], \ldots, l_p[p-1])\) of \( p \) bit vectors of length 64. The \( k \)th bit in \( l_p[i] \) is 0 if and only if \((\frac{-i-km}{p}) = 1\).
  \item \textbf{Step 4:} In a quadruple loop run over the cartesian product of the three lists computed in Step 2 and \( \{3, 4, 8, 11 \text{ mod } 16\} \) and do the following:
    \begin{enumerate}
      \item Use the Chinese remainder theorem to find the unique integer \( 0 \leq r < m \) congruent to the given residues modulo \( m_1, m_2, m_3, 16 \).
      \item Do a logical \textbf{and} of the bit vectors \( l_p[r \text{ mod } p] \) for all prime \( p \) with \( 53 \leq p \leq 197 \).
      \item If the \( k \)th bit of the resulting bit vector is 1, the field \( \mathbb{Q}(\sqrt{-r - km}) \) is suspicious.
      \item Compute the smallest split prime \( p \) for each suspicious field \( \mathbb{Q}(\sqrt{D}) \). If \( 4p^8 > |D| \) then print the field.
    \end{enumerate}
\end{itemize}
\end{algorithm}
Remark 23. The algorithm above finds all the imaginary quadratic fields \( \mathbb{Q}(\sqrt{D}) \) with \(|D| < 3.14 \cdot 10^{20}\), no split prime \( \leq 197 \). We print out only those fields that may have a class group exponent \( \leq 8 \). The run time on a single core on an Intel i5 processor is about 40 days. However, we can execute the loop over the cartesian product in parallel. The result is as follows:

- The algorithm above results in 1002279 imaginary quadratic fields.
- None of them has a class group of exponent \( \leq 100 \).

It will not be easy to extend the programs to higher exponent. We tried the methods of Remarks 20 and exponent 9 for primes \( p \leq 137 \) and this took already two hours. This has to be compared with exponent 8 and \( p \leq 197 \) which was done in about four minutes. The method of Remarks 20 for exponent 9 and \( p > 137 \) cannot be used directly with the 64-bit arithmetic of the processor. As the use of software implemented integers is considerably slower, we could try to adapt the sieve (Algorithm 22) instead. This would mean to search for all fields with smallest split prime \( \geq 137 \) and \( D < 3.14 \cdot 10^{20} \). But, having 12 primes less available for the sieve would result in an impractically long list of fields printed for later inspection.

References

[BS] E. Bach and J. Sorenson, Explicit bounds for primes in residue classes, Math. Comput. 65 (1996), 1717–1735.

[BK] D. W. Boyd and H. Kisilevsky, On the exponent of the ideal class groups of complex quadratic fields, Proc. Amer. Math. Soc. 31 (1972), 433–436.

[BM] M. Boy and G. Malle, A Database for Class Groups of Number Fields, http://www.mathematik.uni-kl.de/~numberfieldtables/KT_2/doc.html.

[C] Y.-G. Chen, On the Siegel–Tatuzawa–Hoffstein theorem, Acta Arith. 130 (2007), 361–367.

[D] M. Deuring, Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins, Invent. Math. 5 (1968), 169-179.

[EK] A. G. Earnest and O. H. Körner, On ideal class groups of 2-power exponent, Proc. Amer. Math. Soc. 86 (1982), 196–198.

[FK] E. Fouvry and J. Klüners, On the 4-rank of quadratic number fields, Invent. Math. 167 (2007), 455–516.

[G] F. Gerth, The 4-class ranks of quadratic fields, Invent. Math. 77 (1989), 489–515.

[HB] D. R. Heath-Brown, Imaginary quadratic fields with class group exponent 5, Forum Math. 20 (2008), 275–283.

[R] L. Rédei, Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, J. Reine Angew. Math. 171 (1938), 55–60.

[S] Y. Sueyoshi, On Rédei matrices with minimal rank, Far East J. Math. Sci. 3 (2001), 121–128.

[T] T. Tatuzawa, On a theorem of Siegel, Japan. J. Math. 21 (1952), 163–178.
Andreas-Stephan Elsenhans  
Universität Würzburg  
Campus Hubland Nord  
Emil-Fischer-Str. 30  
97074 Würzburg, Germany  
E-mail: stephan.elsenhans@mathematik.uni-wuerzburg.de

Jürgen Klüners  
Institut für Mathematik  
Fakultät EIM  
Universität Paderborn  
Warburger Str. 100  
33098 Paderborn, Germany  
E-mail: klueners@math.uni-paderborn.de

Florin Nicolae  
“Simion Stoilow” Institute of Mathematics  
of the Romanian Academy  
P.O. Box 1-764  
RO-014700 Bucureşti, Romania  
E-mail: florin.nicolae@imar.ro