COMPUTING THE TORSION OF THE $p$-RAMIFIED MODULE OF A NUMBER FIELD

FRÉDÉRIC PITOUN AND FIRMIN VARESCON

Abstract. We fix a prime number $p$ and a number field $K$, and denote by $M$ the maximal abelian $p$-extension of $K$ unramified outside $p$. Our aim is to study the $\mathbb{Z}_p$-module $X = \text{Gal}(M/K)$ and to give a method to effectively compute its structure as a $\mathbb{Z}_p$-module. We also give numerical results, for real quadratic fields, cubic fields and quintic fields, together with their interpretations via Cohen-Lenstra heuristics.

1. Introduction

We fix a prime number $p$ and a number field $K$. We denote by $M$ the maximal abelian $p$-extension of $K$ unramified outside $p$. The aim of this paper is to study the $\mathbb{Z}_p$-module $X = \text{Gal}(M/K)$ and give an algorithm to compute its $\mathbb{Z}_p$-structure. This module is described by the exact sequence

$$
\mathcal{U}_K \longrightarrow \prod_{v|p} U_v^1 \longrightarrow X \longrightarrow \text{Gal}(\mathcal{H}/K) \longrightarrow 1,
$$

from class field theory [Gra03, p. 294], where $\mathcal{U}_K$ is the pro-$p$-completion of the group of units $U_K$, $U_v^1$ is the group of principal units at the place $v$ above $p$ of $K$, and $\mathcal{H}$ is the maximal $p$-sub-extension of the Hilbert class field of $K$. Leopoldt’s conjecture for $K$ and $p$ is equivalent to injectivity of $\mathcal{U}_K \rightarrow \prod_{v|p} U_v^1$. Therefore, from this exact sequence, we deduce that the $\mathbb{Z}_p$-rank $r$ of $X$ is greater or equal to $r_2 + 1$ and is equal $r_2 + 1$ if and only if $K$ and $p$ satisfy Leopoldt’s conjecture. Hence $X$ is the direct product of a free part isomorphic to $\mathbb{Z}_p^r$ and of a torsion part, that we denote by $T_p$. Our algorithm checks whether $K$ satisfies Leopoldt’s conjecture at $p$ and then computes the torsion $T_p$.

We propose a method which is based on the fact that the $\mathbb{Z}_p$-module $X$ is the projective limit of the $p$-parts of the ray class groups modulo $p^n$, $\mathcal{A}_p^n(K)$. We then study the stabilization of these groups with respect to $n$ and the behaviour of invariants of $\mathcal{A}_p^n(K)$, as $n$ is increasing. This approach leads us to our algorithm.

Before addressing the technical part of this article, we recall the definition and some basic properties of the ray class groups modulo $p^n$. Then, we use our algorithm to compute some cases and propose an heuristic explanation of the statistical data, using the Cohen-Lenstra philosophy [CL84].

Received by the editor April 10, 2012 and, in revised form, February 13, 2013, April 4, 2013 and May 3, 2013.

2010 Mathematics Subject Classification. Primary 11R23, 11R37, 11Y40.

©2014 American Mathematical Society
2. Background from class field theory

In this section, we recall the basic notions from class field theory that we will need later. We fix $v$ a place of $K$ above $p$ and $\pi_v$ a local uniformiser of $K_v$, the completion of $K$ at $v$. We use [Gra03] and [Ser68] as the main references.

**Definition 2.1.**

1. The conductor of an abelian extension of local fields $L_v/K_v$ is the minimum of integers $c$ such that $U_c^v \subset N_{L_v/K_v}(L_v^\times)$ (we recall that $U_0^v = 1 + (\pi_v^c)$ and we use the convention $U_0^v = U_v$).
2. (Theorem and Definition 4.1 + Lemma 4.2.1 [Gra03] pp. 126–127). The conductor of an abelian extension $L/K$ of a global field is the ideal $m = \prod_v p_v^{c_v}$, where $v$ runs through all finite places of $K$ and where $c_v$ is the conductor of the local extension $L_v/K_v$.

We start with two lemmas.

**Lemma 2.2 ([Ser68] Proposition 9, p. 219]).** Let $K_v$ be the completion of $K$ at the valuation $v$ normalized by $v(p) = 1$ and $v(\pi_v) = \frac{1}{e_v}$, where $e_v$ is the ramification index of the extension $K_v/\mathbb{Q}_p$. If $m > \frac{e_v}{p-1}$, then the map $x \mapsto x^p$ is an isomorphism from $U_v^m$ to $U_v^{m+e_v}$.

**Lemma 2.3.** Let $K_v \subset L_v \subset M_v$ be a tower of extensions of $\mathbb{Q}_p$, such that the extension $M_v/K_v$ is abelian and the extension $M_v/L_v$ is of degree $p$. We denote, respectively, by $c_{M,v}$ and $c_{L,v}$ the conductors of the extensions $M_v/K_v$ and $L_v/K_v$. If $c_{L,v} > \frac{e_v}{p-1}$, then we have

$$c_{M,v} \leq c_{L,v} + e_v.$$

**Proof.** By definition, $c_{L,v}$ is the smallest integer $n$ such that $U_v^n \subset N_{L_v/K_v}(L_v^\times)$. Local class field theory gives the diagram

\[
\begin{array}{cccccc}
1 & \rightarrow & N_{M_v/K_v}(M_v^\times) & \rightarrow & K_v^\times & \rightarrow & \text{Gal}(M_v/K_v) & \rightarrow & 1 \\
& & \searrow & & \downarrow & & \downarrow & & \\
1 & \rightarrow & N_{L_v/K_v}(L_v^\times) & \rightarrow & K_v^\times & \rightarrow & \text{Gal}(L_v/K_v) & \rightarrow & 1
\end{array}
\]

Applying the snake lemma we get the exact sequence

$$1 \rightarrow N_{M_v/K_v}(M_v^\times) \rightarrow N_{L_v/K_v}(L_v^\times) \rightarrow \text{Gal}(M_v/L_v) = \mathbb{Z}/p\mathbb{Z} \rightarrow 1.$$

Consequently, $N_{M_v/K_v}(M_v^\times)$ is a subgroup of $N_{L_v/K_v}(L_v^\times)$ of index $p$. Let $n \in \mathbb{N}$, $n \geq c_{L,v} + e_v$, and $x \in U_v^n$. We have to show that $x \in N_{M_v/K_v}(M_v^\times)$. By Lemma 2.2, $x^{\frac{1}{p}}$ is a well-defined element of $U_v^{n-e_v}$. Yet $n - e_v \geq c_{L,v}$, therefore, $x^{\frac{1}{p}} \in N_{L_v/K_v}(L_v^\times)$. Now, as $N_{M_v/K_v}(M_v^\times)$ is of index $p$ in $N_{L_v/K_v}(L_v^\times)$, we deduce that $x \in N_{M_v/K_v}(M_v^\times)$. Therefore, we have that $U_v^n \subset N_{M_v/K_v}(M_v^\times)$ for all integers $n$ such that $n \geq c_{L,v} + e_v$. By the definition of the conductor, this proves [2].

**Definition 2.4.** Let $n$ be a positive integer. We denote by

- $H$ the maximal abelian unramified extension of $K$;
• $H_{p^n}$ the compositum of all abelian extensions of $K$ whose conductors divide $p^n$;
• $H_{p^n}$ the compositum of all abelian $p$-extensions of $K$ whose conductors divide $p^n$;
• $M$ the maximal extension of $K$ which is abelian and unramified outside $p$.
So the Galois groups $\text{Gal}(H/K)$ and $\text{Gal}(H_{p^n}/K)$ are, respectively, isomorphic to the $p$-parts of $\text{Gal}(H/K)$ and $\text{Gal}(H_{p^n}/K)$.

**Proposition 2.5** ([Gr03, Corollary 5.1.1, p. 47]). We have the exact sequences

$$1 \longrightarrow K^\times \prod_{v \mid p} U_v \prod_{v \mid p} U_v^{ne_v} \longrightarrow \mathcal{I}_K \longrightarrow \text{Gal}(H_{p^n}/K) \longrightarrow 1$$

$$1 \longrightarrow K^\times \prod_v U_v \longrightarrow \mathcal{I}_K \longrightarrow \text{Gal}(H/K) \longrightarrow 1,$$

where $\mathcal{I}_K$ is the group of idèles of $K$.

We denote the Galois group $\text{Gal}(H_{p^n}/K)$ by $A_{p^n}(K)$. It is the $p$-part of the Galois group $\text{Gal}(H_{p^n}/K)$ which, in turn, is isomorphic to the ray class group modulo $p^n$ of $K$. By definition, we have a natural inclusion $H_{p^n} \subset H_{p^{n+1}}$, the union $\bigcup_n H_{p^n}$ is equal to $M$ and the projective limit $\varprojlim_n A_{p^n}(K)$ is canonically isomorphic to $\mathfrak{X}$.

**Proposition 2.6.** For any integer $n > 0$, the Galois groups of the extensions $M$ and $H_{p^n}$ of $K$ are related by the exact sequence

$$1 \longrightarrow U^{(p^n)}_K \longrightarrow \prod_{v \mid p} U_v^{ne_v} \longrightarrow \text{Gal}(M/K) \longrightarrow \text{Gal}(H_{p^n}/K) \longrightarrow 1,$$

where $U^{(p^n)}_K = \{ u \in U_K \text{ such that } \forall v | p, \ u \in U_v^{ne_v} \}$ and

$$\overline{U}_K^{(p^n)} \longrightarrow \prod_{v \mid p} U_v^{ne_v} \longrightarrow \mathfrak{X} \longrightarrow A_{p^n}(K) \longrightarrow 1,$$

where $\overline{U}_K^{(p^n)}$ is the pro-$p$-completion of $U^{(p^n)}_K$, i.e., $\varprojlim_m U^{(p^n)}_K/p^m$. If, moreover, $K$ and $p$ satisfy Leopoldt’s conjecture, then $\overline{U}_K^{(p^n)} \to \prod_{v \mid p} U_v^{ne_v}$ is injective.

**Proof.** To obtain the second exact sequence, we apply the pro-$p$-completion process to the first. Note that the injectivity of $\overline{U}_K^{(p^n)} \to \prod_{v \mid p} U_v^{ne_v}$ is equivalent to Leopoldt’s conjecture. Now we prove exactness of the first sequence.

From the definition of the extensions $M$ and $H_{p^n}$, we deduce the commutative diagram

$$1 \longrightarrow K^\times \prod_{v \mid p} U_v \prod_{v \mid p} 1 \longrightarrow \mathcal{I}_K \longrightarrow \text{Gal}(M/K) \longrightarrow 1$$

$$1 \longrightarrow K^\times \prod_{v \mid p} U_v \prod_{v \mid p} U_v^{ne_v} \longrightarrow \mathcal{I}_K \longrightarrow \text{Gal}(H_{p^n}/K) \longrightarrow 1.$$

By the snake lemma, we have that

$$\ker(\text{Gal}(M/K) \to \text{Gal}(H_{p^n}/K)) = (K^\times \prod_{v \mid p} U_v \prod_{v \mid p} U_v^{ne_v})/(K^\times \prod_{v \mid p} U_v \prod_{v \mid p} 1).$$
Now, we define the map
\[
\theta : (K^\times \prod_{v|p} U_v \prod_{v\nmid p} U_v^{n_{ev}}) \to (\prod_{v|p} U_v^{n_{ev}})/U_K^{(p^n)},
\]
by setting for \( k(u_v) \in K^\times \prod_{v|p} U_v \prod_{v\nmid p} U_v^{n_{ev}}, \) \( \theta(k(u_v)) = (u_v)_{v|p}, \) where \( (u_v)_{v|p} \)

is the class of \((u_v)_{v|p} \) in \((\prod_{v|p} U_v^{n_{ev}})/U_K^{(p^n)}\).

We first check that the map \( \theta \) is well defined, i.e., that if \( k(u_v) = k'(u'_v) \) in \( K^\times \prod_{v|p} U_v \prod_{v\nmid p} U_v^{n_{ev}}, \) then \( \theta(k(u_v)) = \theta(k'(u'_v)). \) By definition, for all \( v, k(u_v) = k'(u'_v) \) if and only if \( i_v(k)u_v = i_v(k')u'_v, \) where \( i_v \) is the embedding of \( K \) in \( K_v. \) We deduce that for all \( v, i_v(k'k^{-1}) \in U_v \) and that for all \( v|p, i_v(k'k^{-1}) \in U_v^{n_{ev}}. \) So we get \( k'k^{-1} \in U_K^{(p^n)} \) and \( (u_v)_{v|p} = (u'_v)_{v|p}. \)

It is clear that \((K^\times \prod_{v|p} U_v \prod_{v\nmid p} 1) \subset \ker(\theta) \) and that the map \( \theta \) is surjective. We will show that \((K^\times \prod_{v|p} U_v \prod_{v\nmid p} 1) = \ker(\theta). \) Let \( k(u_v) \in \ker(\theta). \) Then there exists \( x \in U_K^{(p^n)} \) such that for all \( v|p, u_v = i_v(x). \) We consider the element \( x(u'_v) \) where \( u'_v = 1 \) if \( v|p \) and \( u'_v = i_v(x)^{-1}u_v \) if \( v \not| p. \) We have \( (u_v)x(u'_v) \Rightarrow k(u_v) = kx(u'_v) \) and as \( kx(u'_v) \in (K^\times \prod_{v|p} U_v \prod_{v\nmid p} 1), \) we have \( \ker(\theta) \subset (K^\times \prod_{v|p} U_v \prod_{v\nmid p} 1), \) and, finally

\[
(K^\times \prod_{v|p} U_v \prod_{v\nmid p} U_v^{n_{ev}})/(K^\times \prod_{v|p} U_v \prod_{v\nmid p} 1) \cong (\prod_{v\nmid p} U_v^{n_{ev}})/U_K^{(p^n)}.
\]

We deduce the first exact sequence. \( \square \)

3. Explicit Computation of \( T_p \)

In this section, we present our method to check that \( K \) satisfies Leopoldt’s conjecture at \( p \) and then to compute \( T_p. \) The main point is that, for \( n \) large enough, \( A_{p^n}(K) \) determines \( X. \)

3.1. Stabilization of \( A_{p^n}(K). \) For simplicity we denote \( Y_n = \ker(A_{p^n+1}(K) \to A_{p^n}(K)). \) Let \( \tilde{K} \) be the compositum of all the \( \mathbb{Z}_p \)-extensions of \( K. \) We denote by \( r \) the \( \mathbb{Z}_p \)-rank of \( X, \) so that \( r \geq r_2 + 1. \)

**Proposition 3.1.** There exists an \( n_0 \) such that \( \tilde{K} \cap H_{p^{n_0}}/\tilde{K} \cap H_p \) is ramified at all places above \( p. \) Also, for all \( n \geq n_0, Y_n \) surjects onto \( (\mathbb{Z}/p\mathbb{Z})^r. \)

Before proving the proposition, we need a lemma.

**Lemma 3.2.** If the extension \( \tilde{K} \cap H_{p^n}/\tilde{K} \cap H_p \) is ramified at a place \( v \) above \( p, \)
then \( c_{n,v} > \frac{e_v}{p-1}, \) where \( c_{n,v} \) is the conductor of the local extension \( (\tilde{K} \cap H_{p^n})_w/\tilde{K}_v \)
and \( w \) is a place above \( v. \)

**Proof of Lemma 3.2.** As \( M \) contains the cyclotomic \( \mathbb{Z}_p^* \)-extension, there exists an \( n_0 \) such that \( \tilde{K} \cap H_{p^{n_0}}/\tilde{K} \cap H_p \) is ramified at all places \( v \) above \( p. \) As \( \tilde{K} \cap H_{p^{n_0}}/\tilde{K} \cap H_p \) is ramified at \( v, \) then, for \( n \geq n_0, \tilde{K} \cap H_{p^n}/\tilde{K} \cap H_p \) is ramified at \( v, \) so that there exists an \( m \) such that \( n \geq m \geq 2 \) and that \( \tilde{K} \cap H_{p^{m-1}}/\tilde{K} \cap H_p \) is unramified at \( v \) and such that \( \tilde{K} \cap H_{p^m}/\tilde{K} \cap H_p \) is ramified at \( v. \) Then the local conductor \( c_{m,v} \) is greater than \( (m-1)e_v, \) yet \( m \geq 2 \) so \( c_{m,v} > (m-1)e_v \geq e_v > \frac{e_v}{p-1}. \) As the conductor of the extension \( \tilde{K} \cap H_{p^n}/K \) divides the conductor of \( \tilde{K} \cap H_{p^n}/K, \) we have \( c_{n,v} \geq c_{m,v} > \frac{e_v}{p-1}. \) \( \square \)
Proof of the Proposition 3.1 We consider the diagram
\[
\begin{array}{ccc}
\mathcal{K} \cap \mathcal{H}_{p^n} & \longrightarrow & (\mathcal{K} \cap \mathcal{H}_{p^n})/\mathcal{H}_p \\
\downarrow & & \downarrow \\
\mathcal{K} \cap \mathcal{H}_{p^{n-1}} & \longrightarrow & (\mathcal{K} \cap \mathcal{H}_{p^{n-1}})/\mathcal{H}_{p^{n-1}} \\
\downarrow & & \downarrow \\
\mathcal{K} \cap \mathcal{H}_p & \longrightarrow & \mathcal{H}_p \\
& & \downarrow \quad Y_{n-1} \\
& & K
\end{array}
\]

We have \(\text{Gal}(\mathcal{K}/\mathbb{K}) = \mathbb{Z}_p^r\). It is clear that \(Y_n \rightarrow \text{Gal}(\mathcal{K} \cap \mathcal{H}_{p^{n+1}})/\mathcal{K} \cap \mathcal{H}_{p^n}\). Yet \(\text{Gal}(\mathcal{K} \cap \mathcal{H}_{p^n})\) is a \(\mathbb{Z}_p\)-submodule of \(\text{Gal}(\mathcal{K}/\mathbb{K}) = \mathbb{Z}_p^r\) of finite index, so it is isomorphic to \(\mathbb{Z}_p^r\). Hence there exist \(r\) extensions, say \(M_1, M_2, \ldots, M_r\) of \(\mathcal{K} \cap \mathcal{H}_{p^n}\), contained in \(\mathcal{K}\) such that \(\text{Gal}(M_i/\mathcal{K} \cap \mathcal{H}_{p^n}) \simeq \mathbb{Z}/p\mathbb{Z}\) and \(\text{Gal}(M_1 \cdots M_r/\mathcal{K} \cap \mathcal{H}_{p^n}) \simeq (\mathbb{Z}/p\mathbb{Z})^r\). Yet the conductor of the extension \(\mathcal{K} \cap \mathcal{H}_{p^n}/\mathcal{K}\) divides \(p^n = \prod_{v \mid p} p_v^{n e_v}\).

Moreover, the hypothesis on \(\mathcal{K} \cap \mathcal{H}_{p^n}/\mathcal{K} \cap \mathcal{H}_p\) ensures that we can use Lemma 2.3 and consequently the conductor of the extension \(M_i/\mathcal{K}\) divides \(\prod_{v \mid p} p_v^{n e_v + e_v}\) = \(p^{n+1}\), i.e., \(M_i \subset \mathcal{H}_{p^{n+1}}\) for all \(i \in \{1, \cdots, r\}\). Hence the map is surjective. \(\square\)

We deduce immediately the corollary.

Corollary 3.3. Let \(n\) be a positive integer such that the extension \(\mathcal{K} \cap \mathcal{H}_{p^n}/\mathcal{K} \cap \mathcal{H}_p\) is ramified at all places above \(p\), and that the cardinality of \(Y_n\) is exactly \(p^{r+1}\). Then \(Y_n \simeq (\mathbb{Z}/p\mathbb{Z})^{r+1}\) and \(K\) satisfies Leopoldt’s conjecture at \(p\).

From now on, as we can numerically check that \(K\) satisfies Leopoldt’s conjecture at \(p\), we assume it does so, in order to compute \(T_p\). Note that if Leopoldt’s conjecture is false, then \(r > r_2 + 1\) and our algorithm never stops.

Corollary 3.4. We assume that, for some integer \(n\) such that the extension \(\mathcal{K} \cap \mathcal{H}_{p^n}/\mathcal{K} \cap \mathcal{H}_p\) is ramified at all places above \(p\), the cardinal of \(Y_n\) is exactly \(p^{r+1}\). Then \(Y_n \simeq \text{Gal}(\mathcal{K} \cap \mathcal{H}_{p^{n+1}})/\mathcal{K} \cap \mathcal{H}_{p^n}\).

It remains to check that if \(Y_{n_0} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}\) for some \(n_0\), then \(Y_n \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}\) for all integers \(n \geq n_0\). For this purpose, we consider the exact sequence defining the \(p\)-part of the ray class group
\[
1 \longrightarrow \mathcal{U}_{K}^{(p^n)} \longrightarrow \prod_{v \mid p} U_v^{n e_v} \longrightarrow \mathcal{X} \longrightarrow A_{p^n}(K) \longrightarrow 1,
\]
and we denote \(Q_n = \prod_{v \mid p} U_v^{n e_v}/\mathcal{U}_{K}^{(p^n)}\). We have \(Q_n = \text{Gal}(M/\mathcal{H}_{p^n})\) and consequently \(Q_n/Q_{n+1} = Y_n \simeq \text{Gal}(\mathcal{H}_{p^{n+1}}/\mathcal{H}_{p^n})\).

Proposition 3.5. For \(n \geq 2\), raising to the \(p\)\textsuperscript{th} power induces, via the Artin map, a surjection from \(Y_n\) to \(Y_{n+1}\).

Proof. Recall that \(Q_n = \prod_{v \mid p} U_v^{n e_v}/\mathcal{U}_{K}^{(p^n)} = \ker(\mathcal{X} \rightarrow A_{p^n}(K))\). We have that \(n > \frac{1}{p-1}\). Raising to the \(p\)\textsuperscript{th} power realizes an isomorphism of \(\prod_{v \mid p} U_v^{n e_v}\) onto
\[ \prod_{v \mid p} U_{v}^{ne_{v} + e_{v}}. \] This isomorphism induces a surjection from \( \mathbb{Q}_{n} \) onto \( \mathbb{Q}_{n+1} \). We consider the diagram

\[
\begin{array}{c}
1 \longrightarrow \mathbb{Q}_{n+1} \longrightarrow \mathbb{Q}_{n} \longrightarrow \mathbb{Q}_{n}/\mathbb{Q}_{n+1} \longrightarrow 1 \\
\downarrow^{(\cdot)^{p}} \quad \downarrow^{(\cdot)^{p}} \quad \downarrow^{(\cdot)^{p}} \\
1 \longrightarrow \mathbb{Q}_{n+2} \longrightarrow \mathbb{Q}_{n+1} \longrightarrow \mathbb{Q}_{n+1}/\mathbb{Q}_{n+2} \longrightarrow 1.
\end{array}
\]

We deduce from the snake lemma that the vertical arrow on the right-hand side is a surjection from \( \mathbb{Q}_{n}/\mathbb{Q}_{n+1} \) onto \( \mathbb{Q}_{n+1}/\mathbb{Q}_{n+2} \), i.e., from \( Y_{n} \) onto \( Y_{n+1} \).

**Corollary 3.6.** We denote \( q_{n} = \#(Y_{n}) \). For all \( n \geq 2 \), \( q_{n} \geq q_{n+1} \). Therefore the sequence \( (q_{n})_{n \geq 1} \) is ultimately constant.

We recall that \( Y_{n} \) is \( \ker(A_{p^{n+1}}(K) \to A_{p^{n}}(K)) \).

**Theorem 3.7.** As we assume Leopoldt’s conjecture, there exists an integer \( n_{0} \) such that \( Y_{n_{0}} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_{2}+1} \). Moreover, for all integers \( n \geq n_{0} \), the modules \( \mathbb{Q}_{n} = \text{Gal}(M/\mathcal{H}_{p^{n}}) \) are \( \mathbb{Z}_{p} \)-free of rank \( r_{2} + 1 \) and

\[ Y_{n} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_{2}+1}. \]

**Proof.** The \( \mathbb{Z}_{p} \)-module \( \mathcal{X} \) is isomorphic to the direct product of its torsion part and of \( \mathbb{Z}_{p}^{r_{2}+1} \). An isomorphism being chosen, we can identify \( \mathbb{Z}_{p}^{r_{2}+1} \) with a subgroup of \( \mathcal{X} \) and therefore define, via Galois theory, an extension \( M' \) of \( K \) such that \( \text{Gal}(M'/K) \simeq T_{p}^{+} \) and \( KM' = M \).

Since this extension is unramified outside \( p \), there exists an integer \( n_{1} \) such that \( M' \subset \mathcal{H}_{p^{n_{1}}} \) and consequently \( \mathcal{H}_{p^{n_{1}}}/K = M' \). Moreover, for all integers \( n \geq n_{1} \), \( \text{Gal}(M/\mathcal{H}_{p^{n}}) \) is a submodule of finite index of \( \text{Gal}(M/M') = \mathbb{Z}_{p}^{r_{2}+1} \), and consequently \( \mathbb{Q}_{n} = \text{Gal}(M/\mathcal{H}_{p^{n}}) \simeq \mathbb{Z}_{p}^{r_{2}+1} \). The \( \mathbb{Z}_{p} \)-module \( \mathbb{Q}_{n} \) is therefore free of rank \( r_{2} + 1 \).

About the other kernel \( Y_{n} \) we saw that there exists an integer \( n_{2} \) such that \( Y_{n} \) maps surjectively onto \( (\mathbb{Z}/p\mathbb{Z})^{r_{2}+1} \) for all integer \( n \geq n_{2} \) (we can choose \( n_{2} \) to be the minimum of all integers \( n \) such that for all \( p \)-places \( v \) the conductors of \( (\mathcal{K} \cap \mathcal{H}_{p^{n}})/K_{v} \) are at least \( \frac{r_{2}+1}{p-1} \)). Then we note that mapping \( x \in U_{v}^{ne_{v}} \) to \( x \in U_{v}^{ne_{v}+e_{v}} \) realizes an isomorphism between \( U_{v}^{ne_{v}} \) and \( U_{v}^{ne_{v}+e_{v}} \), so that the quotient \( \mathbb{Q}_{n}/\mathbb{Q}_{n+1} \), which is isomorphic to \( Y_{n} \), is killed by \( p \). Define \( n_{0} = \text{Max}(n_{1}, n_{2}) \) and let \( n \geq n_{0} \) be an integer. The kernel \( Y_{n} \) is therefore a quotient of \( \mathbb{Z}_{p}^{r_{2}+1} \), which maps surjectively onto \( (\mathbb{Z}/p\mathbb{Z})^{r_{2}+1} \) and is killed by \( p \). Hence we get \( Y_{n} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_{2}+1} \).

### 3.2. Computing the invariants of \( T_{p} \)

We start by recalling the definition of the invariant factors of an abelian group \( G \).

**Definition 3.8.** Let \( G \) be a finite abelian group, there exists a unique sequence \( a_{1}, \ldots, a_{t} \) such that \( a_{i}|a_{i+1} \) for \( i \in \{1, \ldots, t-1\} \) and \( G \simeq \prod_{i=1}^{t} \mathbb{Z}/a_{i}\mathbb{Z} \). These \( a_{i} \) are the invariant factors of the group \( G \).

In what follows we will denote these invariants by \( \mathcal{FI}(G) = [a_{1}, \ldots, a_{t}] \). If \( G \) is a \( p \)-group, these invariant factors are all powers of \( p \). In practice, we are able to determine the invariant factors of \( A_{p^{n}}(K) \). We will see in this section that the knowledge of invariant factors of \( A_{p^{n}}(K) \), for \( n \) large enough, combined with the stabilizing properties of \( A_{p^{n}}(K) \), does determine explicitly the invariant factors of \( T_{p} \), and thus \( T_{p} \) itself. We recall that for \( n \) large enough, \( A_{p^{n}}(K) \) is isomorphic to
the direct product of \( \text{Gal}(\tilde{K} \cap \mathcal{H}_{p^n}) / K) \) and of \( \text{Gal}(\mathcal{H}_{p^n} / \tilde{K} \cap \mathcal{H}_{p^n}) = T_p \). So we will first explore the structure of \( \text{Gal}(\tilde{K} \cap \mathcal{H}_{p^n} / K) \).

**Proposition 3.9.** Let \( n_0 \) be such that \( \tilde{K} \cap \mathcal{H}_{p^{n_0}} / \tilde{K} \cap \mathcal{H}_p \) is ramified at all places above \( p \) and

\[
Y_{n_0} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}.
\]

Then for all integers \( n \geq n_0 \), we have

\[
\text{Gal}(\tilde{K} / \tilde{K} \cap \mathcal{H}_{p^{n+1}}) = p \text{Gal}(\tilde{K} / \tilde{K} \cap \mathcal{H}_{p^n}).
\]

**Proof.** By Theorem 3.7, on the one hand, \( Q_n \) is \( \mathbb{Z}_p \)-free of rank \( r_2 + 1 \) and, on the other hand, \( Y_n = Q_n / Q_{n+1} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1} \). This gives \( Q_{n+1} = pQ_n \). As \( \tilde{K} \cap \mathcal{H}_{p^{n_0}} / \tilde{K} \cap \mathcal{H}_p \) is ramified at all places above \( p \) and \( Y_{n_0} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1} \), we have \( T_p \subset A_{p^{n_0}}(K) \), so \( \tilde{K} \mathcal{H}_{p^{n_0}} = M \). Then, considering the diagram

\[
\begin{array}{ccc}
\tilde{K} & \xrightarrow{Q_{n+1}} & M \\
\downarrow & & \downarrow \\
\tilde{K} \cap \mathcal{H}_{p^{n+1}} & \xrightarrow{H_{p^{n+1}}} & \mathcal{Q}_n \\
\downarrow & & \downarrow \\
\tilde{K} \cap \mathcal{H}_{p^n} & \xrightarrow{H_{p^n}} & \mathcal{Q}_n \\
\downarrow & & \downarrow \\
K & & K
\end{array}
\]

we get the required isomorphism. \( \square \)

**Corollary 3.10.** Let \( n_0 \) be an integer such that \( \tilde{K} \cap \mathcal{H}_{p^{n_0}} / \tilde{K} \cap \mathcal{H}_p \) is ramified at all places above \( p \) and such that \( Y_{n_0} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1} \). Then for all integers \( n \geq n_0 \) the invariant factors of \( \text{Gal}(\tilde{K} \cap \mathcal{H}_{p^{n+1}} / K) \) are obtained by multiplying by \( p \) each invariant factor of \( \text{Gal}(\tilde{K} \cap \mathcal{H}_{p^n} / K) \).

From the fact that \( A \simeq \mathbb{Z}_p^{r_2+1} \times T_p \), the ray class group, \( \text{Gal}(\mathcal{H}_{p^n} / K) \), is isomorphic to the direct product of \( \text{Gal}(\tilde{K} \cap \mathcal{H}_{p^n} / K) \) and \( \text{Gal}(\mathcal{H}_{p^n} / \tilde{K} \cap \mathcal{H}_{p^n}) \). The invariant factors of \( \text{Gal}(\mathcal{H}_{p^n} / K) \) are then simply obtained by concatenating the two groups forming the direct product. We now state the result that explicitly determines \( T_p \).

**Theorem 3.11.** Let \( n \) be such that \( Y_n = (\mathbb{Z}/p\mathbb{Z})^{r_2+1} \) and \( \tilde{K} \cap \mathcal{H}_{p^n} / \tilde{K} \cap \mathcal{H}_p \) is ramified at all places above \( p \). We assume that

\[
\mathcal{FI}(A_{p^n}(K)) = [b_1, \ldots, b_t, a_1, \ldots, a_{r_2+1}]
\]

with \( (v_p(a_1)) > (v_p(b_1)) + 1 \), and that

\[
\mathcal{FI}(A_{p^{n+1}}(K)) = [b_1, \ldots, b_t, pa_1, \ldots, pa_{r_2+1}].
\]

Then we have

\[
\mathcal{FI}(T_p) = [b_1, \ldots, b_t].
\]
Proof. Indeed, as $Y_n \simeq (\mathbb{Z}/p\mathbb{Z})^{2+1}$, we have $A_p^n(K) \simeq T_p \times \text{Gal}(\bar{K} \cap \mathcal{H}_p^n/K)$ for $i \in \{n, n+1\}$. We saw that the invariant factors of $\text{Gal}(\bar{K} \cap \mathcal{H}_p^n/K)$ are exactly equal to $p$ times those of $\text{Gal}(\bar{K} \cap \mathcal{H}_p^n/K)$. Consequently, if $a$ is an invariant factor of $\text{Gal}(\bar{K} \cap \mathcal{H}_p^n/K)$, we have necessarily that $a = pa$ or $a = pb$. But as $\text{Min}(v_p(a_i)) > \text{Max}(v_p(b_i)) + 1$, none of the invariant factors of $\text{Gal}(\bar{K} \cap \mathcal{H}_p^n/K)$ are of the form $pb$. The invariant factors of $\text{Gal}(\bar{K} \cap \mathcal{H}_p^n/K)$ are therefore exactly $pa_1^r, \ldots, pa_{r+1}^r$. The result follows from the fact that $A_p^n(K)$ is isomorphic to the direct product of $T_p$ and $\text{Gal}(\bar{K} \cap \mathcal{H}_p^n/K)$. □

4. Explicit computation of bounds

More generally, if we denote by $e = \max_{v | p} \{e_v\}$ the ramification index of $K/\mathbb{Q}$ and by $s$ the $p$-adic valuation of $e$, then we can start to check whether $A_p^n(K)$ stabilizes from rank $n = 2 + s$. To show that $n = 2 + s$ is the proper starting point we consider the diagram

$$
\begin{array}{c}
\tilde{K} \cap \mathcal{H}_p \\
K
\end{array}
\begin{array}{c}
\tilde{K} \cap \mathcal{H}_p^n \\
K_{s+1}
\end{array}
\begin{array}{c}
\mathcal{H}_p \\
\mathcal{H}_p^{n+1}
\end{array}
\begin{array}{c}
\mathcal{H}_p^{r+2} \\
\mathcal{H}_p^{s+2}
\end{array}
$$

where $K_j$ is the $j^{th}$ field of the $\mathbb{Z}_p$-extension of $K$.

We prove below that the places above $p$ are totally ramified in $K_{s+1}/K_s$. Therefore, $\tilde{K} \cap \mathcal{H}_p^n/K \cap \mathcal{H}_p$ is ramified at all places above $p$ and we start the computation by checking whether $A_p^n(K)$ stabilizes from $n = s + 2$, and until it stabilizes. We first prove that all places above $p$ are totally ramified in $K_{s+1}/K_s$.

We consider the diagram

$$
\begin{array}{c}
K_{s+1} \\
K_s
\end{array}
\begin{array}{c}
\mathbb{Q}_{s+1} \\
\mathbb{Q}_s
\end{array}
\begin{array}{c}
\mathbb{Q} \\
K
\end{array}
$$

The ramification index of $p$ in $\mathbb{Q}_{s+1}/\mathbb{Q}$ is $p^{s+1}$, while the one in $K/\mathbb{Q}$ is $p^s a$ with $p \nmid a$. Therefore the extension $K_{s+1}/K$ is ramified and $K_{s+1}/K_s$ is totally ramified at all places above $p$. 
Corollary 4.1. Let $e$ be the ramification index of $p$ in $K/\mathbb{Q}$ and let $s$ be the $p$-adic valuation of $e$. Let $n \geq 2 + s$, we assume that

$$\mathcal{FI}(A_p^n(K)) = [b_1, \ldots, b_t, a_1, \ldots, a_{t^2+1}],$$

with $\text{Min}(v_p(a_i)) > \text{Max}(v_p(b_i)) + 1$ and, moreover, that

$$\mathcal{FI}(A_p^{n+1}(K)) = [b_1, \ldots, b_t, pa_1, \ldots, pa_{t^2+1}].$$

Then we have

$$\mathcal{FI}(\mathcal{T}_p) = [b_1, \ldots, b_t].$$

All the computations have been done using the PARI/GP system [PAR13].

Example 4.2. We consider the field $K = \mathbb{Q}(\sqrt{-129})$ and $p = 3$. We have $\mathcal{FI}(A_p^2(K)) = [3, 3, 9]$, $\mathcal{FI}(A_p^3(K)) = [3, 9, 27]$ and $\mathcal{FI}(A_p^4(K)) = [3, 27, 81]$. We deduce that $\mathcal{T}_p = (\mathbb{Z}/3\mathbb{Z})$.

5. Numerical results

In the section, we present some of our numerical results and give an explanation of these computations.

5.1. Heuristic approach. We first recall some results on Cohen-Lenstra Heuristics. The main reference on the subject is the seminal paper of Cohen-Lenstra [CL84]; see also [Del07]. These heuristics leads us to compare the proportion of fields with non-trivial $\mathcal{T}_p$ with the proportion of groups with non-trivial $p$-part inside all finite abelian groups. If we assume that the extension $K/\mathbb{Q}$ is Galois with $\Delta = \text{Gal}(K/\mathbb{Q})$, then the module $\mathcal{T}_p$ is a $\mathbb{Z}[\Delta]$-module. In this section, we assume that $\Delta$ is cyclic of cardinality $l$, for some prime number $l$. Then, as the $p$-part of the class group, $\mathcal{T}_p$ itself is a finite $O_l$-module, where $O_l$ is the ring of integers of $\mathbb{Q}(\zeta_l)$. This module $\mathcal{T}_p$ is known in Iwasawa theory as the proper $p$-adic analogue of the class group. Hence it is a natural question to compute it, to examine the distribution of fields with non-trivial $\mathcal{T}_p$, and to compare this distribution with the Cohen-Lenstra heuristics about the distribution of groups with non-trivial $p$-part inside all finite abelian groups.

In what follows, $O_F$ will be the ring of integers of a number field and $G$ will be a finite $O_F$-module. In general, we know that all $O_F$-modules $G$ can be written in a non-canonical way as $\bigoplus_{i=1}^g O_F/a_i$, where the $a_i$ are ideals of $O_F$. Yet the Fitting ideal $a = \prod_{i=1}^g a_i$ depends only on the isomorphism class of $G$, considered as a $O_F$-module. This invariant, denoted by $a(G)$, can be considered as a generalization of the order of $G$. We also have $N(a(G)) = \#G$.

We consider a function $g$, defined on the set of the isomorphism classes of $O_F$-modules (typically $g$ is a characteristic function). We follow [CL84] for the next definition, using the same notations.

Definition 5.1. The average of $g$, if it exists, is the limit when $N \to \infty$ of the quotient

$$\frac{\sum_{G, N(a(G)) \leq N} g(G)}{\sum_{G, N(a(G)) \leq N} 1 / \#\text{Aut}_{O_F}(G)}.$$
where $\sum_{G,N(a(G)) \leq N}$ is the sum is over all isomorphism classes of $O_F$-modules $G$. This average is denoted by $M_{l,0}(g)$.

We denote by $w(a) = \sum_{G,a(G)=a} \frac{1}{\# \text{Aut}_{O_F}(G)}$, where $a$ is an ideal of $O_F$ (using the same notation as [CL84]).

**Proposition 5.2 ([CL84] Corollary 3.8, p. 40).** Let $n \in \mathbb{N}$. Then

$$w(a) = \frac{1}{N(a)} \left( \prod_{p^a|a} \prod_{k=1}^{\alpha} \left( 1 - \frac{1}{N_{O_F}(p)k} \right) \right)^{-1}.$$  

The notation $p^a|a$ means that $p^a|a$ and that $p^a+1 \nmid a$. Consequently, the function $w$, defined on the set of ideals of $O_F$, is multiplicative.

**Notation.** We denote by $\Pi_p$ the characteristic function of the set of isomorphism classes of groups whose $p$-part is non-trivial.

**Proposition 5.3 ([CL84] Example 5.10, p. 47).** We denote by $p_1, \cdots, p_g$ the $p$-places of $O_F$, the average of $\Pi_p$ exists and we have

$$(4) \quad M_{l,0}(\Pi_p) = 1 - \prod_{i=1}^{g} \prod_{k \geq 1} \left( 1 - \frac{1}{p_i^{kf_i}} \right),$$

where $f_i$ is the degree of the residual extensions $O_F/p_i$ over $\mathbb{F}_p$.

**Corollary 5.4.** If the extension $F$ is a Galois extension, all residual degrees are equal to $f$ and in this case

$$M_{l,0}(\Pi_p) = 1 - \prod_{k \geq 1} \left( 1 - \frac{1}{p^{kf}} \right)^g.$$  

**Remark.** The real number $M_{l,0}(\Pi_p)$ is called the 0-average. This notion can be generalized to the $u$-average. The expression to compute the $u$-average is obtained by replacing $k$ by $k + u$ in the expression (4) of the 0-average.

Let $K$ be a set of number fields, cyclic of degree $l$, let $K$ run through $K$ and let $G$ be the $p$-part of the class group of $F$. We assume $l \neq p$. If we denote by $A = \mathbb{Z}[\Delta]/\sum_{g \in \Delta} g$, where $\Delta = \text{Gal}(K/\mathbb{Q})$, it is easy to see that $G$ is a finite $A$-module. As $\Delta$ is cyclic of order $l$, then $G$ is an $O_l$-module. Following the Cohen-Lenstra Heuristics we give the assumptions.

**Assumptions 1 ([CL84] Assumptions, p. 54).** Recall that $l = [K : \mathbb{Q}]$, then we have:

1. (Complexe quadratic case) If $r_1 = 0$, $r_2 = 1$, then the proportion of $G$ which are non-trivial is the 0-average of $\Pi_p$, restricted to $O_l$-modules of order prime to $l$.
2. (Totally real case) If $r_1 = n$, $r_2 = 0$, then the proportion of $G$ which are non-trivial is the 1-average of $\Pi_p$, restricted to $O_l$-modules of order prime to $l$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
5.2. Some numerical results.

5.2.1. Case of the quadratic fields. We observed that in the case of real quadratic fields the proportion of fields with non-trivial $\mathbb{Z}_p$-torsion of $X$ was a 0-average, and a 1-average for the imaginary quadratic fields. We will explain why this phenomenon is consistent with Cohen-Lenstra Heuristics in Section 5.2.2.

We consider all quadratic fields $\mathbb{Q}(\sqrt{d})$ with $d$ square-free and $0 < d \leq 10^9$. Then we compute the proportion of fields with non-trivial $\mathcal{T}_p$. We denote this proportion by $f_{\text{exp}}$. The relative error $|f_{\text{exp}} - M_{2,0}(\Pi_p)|/M_{2,0}(\Pi_p)$ is denoted by $\delta$. We remark that $\delta$ tends to 0 if we increase the numbers of fields whose torsion we compute, except for the cases $p=2$ and 3. We explain this discrepancy with 2 and 3 in Section 5.2.2.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$M_{2,0}(\Pi_p)$</th>
<th>$f_{\text{exp}}$</th>
<th>$\delta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.71118</td>
<td>0.93650</td>
<td>0.31683</td>
</tr>
<tr>
<td>3</td>
<td>0.43987</td>
<td>0.50120</td>
<td>0.13942</td>
</tr>
<tr>
<td>5</td>
<td>0.23967</td>
<td>0.23854</td>
<td>0.00470</td>
</tr>
<tr>
<td>7</td>
<td>0.16320</td>
<td>0.16280</td>
<td>0.00247</td>
</tr>
<tr>
<td>11</td>
<td>0.09916</td>
<td>0.09893</td>
<td>0.00243</td>
</tr>
<tr>
<td>13</td>
<td>0.08284</td>
<td>0.08266</td>
<td>0.00212</td>
</tr>
<tr>
<td>17</td>
<td>0.06228</td>
<td>0.06214</td>
<td>0.00233</td>
</tr>
<tr>
<td>19</td>
<td>0.05540</td>
<td>0.05526</td>
<td>0.00260</td>
</tr>
<tr>
<td>23</td>
<td>0.04537</td>
<td>0.04527</td>
<td>0.00207</td>
</tr>
<tr>
<td>29</td>
<td>0.03375</td>
<td>0.03560</td>
<td>0.00193</td>
</tr>
<tr>
<td>31</td>
<td>0.03330</td>
<td>0.03323</td>
<td>0.00219</td>
</tr>
<tr>
<td>37</td>
<td>0.02776</td>
<td>0.02770</td>
<td>0.00198</td>
</tr>
<tr>
<td>41</td>
<td>0.02499</td>
<td>0.02493</td>
<td>0.00207</td>
</tr>
<tr>
<td>43</td>
<td>0.02380</td>
<td>0.02376</td>
<td>0.00152</td>
</tr>
<tr>
<td>47</td>
<td>0.02173</td>
<td>0.02168</td>
<td>0.00207</td>
</tr>
</tbody>
</table>

We consider now the quadratic field $\mathbb{Q}(\sqrt{d})$ with $-10^9 \leq d \leq 0$. One uses the 1-average denoted by $M_{2,1}(\Pi_p)$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$M_{2,1}(\Pi_p)$</th>
<th>$f_{\text{exp}}$</th>
<th>$\delta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.42235</td>
<td>0.93650</td>
<td>1.12734</td>
</tr>
<tr>
<td>3</td>
<td>0.15981</td>
<td>0.25718</td>
<td>0.60926</td>
</tr>
<tr>
<td>5</td>
<td>0.04958</td>
<td>0.04909</td>
<td>0.00989</td>
</tr>
<tr>
<td>7</td>
<td>0.02374</td>
<td>0.02365</td>
<td>0.00374</td>
</tr>
<tr>
<td>11</td>
<td>0.00908</td>
<td>0.00905</td>
<td>0.00416</td>
</tr>
<tr>
<td>13</td>
<td>0.00641</td>
<td>0.00638</td>
<td>0.00360</td>
</tr>
<tr>
<td>17</td>
<td>0.00368</td>
<td>0.00365</td>
<td>0.00445</td>
</tr>
<tr>
<td>19</td>
<td>0.00292</td>
<td>0.00291</td>
<td>0.00589</td>
</tr>
<tr>
<td>23</td>
<td>0.00198</td>
<td>0.00197</td>
<td>0.00510</td>
</tr>
<tr>
<td>29</td>
<td>0.00123</td>
<td>0.00122</td>
<td>0.00916</td>
</tr>
<tr>
<td>31</td>
<td>0.00108</td>
<td>0.00107</td>
<td>0.00929</td>
</tr>
<tr>
<td>37</td>
<td>0.00075</td>
<td>0.00074</td>
<td>0.00813</td>
</tr>
<tr>
<td>41</td>
<td>0.00061</td>
<td>0.00060</td>
<td>0.00982</td>
</tr>
<tr>
<td>43</td>
<td>0.00055</td>
<td>0.00055</td>
<td>0.00998</td>
</tr>
<tr>
<td>47</td>
<td>0.00046</td>
<td>0.00046</td>
<td>0.01626</td>
</tr>
</tbody>
</table>
We have also computed the proportions for cubic fields, with the program of K. Belabas [Bel97], and for quintic fields using the tables which are available on the website dedicated to PARI/GP system [PAR13]. Then we consider the distribution of torsion modules with respect to invariant factors that will not be presented here, for the sake of brevity. To compute \( \# \text{Aut}_{O_K}(G) \) we use [Hal38].

5.2.2. Explanation of numerical results. In this section we explain our numerical results. Looking at the two tables in §5.2.1 we remark that the proportion \( f_{\exp} \) for real quadratic fields seems to be a 0-average, and a 1-average for the imaginary quadratic. We remark also that the default \( \delta \) for \( p = 2, 3 \) increases with the number of fields computed. To explain these phenomena we recall a computation of Gras [Gra82, pp. 94–97]. Let \( k \) be a number field, we denote by \( K = k(\zeta_p) \) and \( \omega \) the idempotent associated with the action of \( \text{Gal}(K/k) \) on \( \mu_p \).

Theorem 5.5 ([Gra82] Corollaire 1, p. 96). Let \( p \) be a prime, \( p \neq 2 \). If \( \mu_p \not\subset k \), then the torsion of \( X \) is trivial if and only if any prime ideal of \( k \) dividing \( p \) is totally split in \( K/k \) and \((\text{Cl}_K)^\omega\) is trivial, where \( \text{Cl}_K \) is the \( p \)-part of the class group of \( K \).

In the case of quadratic fields, if \( p > 3 \), then \( \mu_p \not\subset k \) and the ramification index of \( p \) in \( \mathbb{Q}(\zeta_p)/\mathbb{Q} \) is \( p - 1 \); then all prime ideals of \( k \) dividing \( p \) ramify in \( K \). Therefore they are not totally split, and so the torsion is trivial if and only if \((\text{Cl}_K)^\omega\) is trivial. So when \( k \) is a real quadratic field the computation of \( T_p \) reduces to the computation of a class group of imaginary quadratic field and we use the 0-average following Cohen-Lenstra Heuristics. In the case of imaginary quadratic the remark [Gra82] pp. 96–97] explains the 1-average. In the case \( p = 3 \), if \( d \equiv 6 \mod 9 \), then the ideal of \( k \) above \( p \) is totally split in \( K \), so the torsion is non-trivial. It explains why the frequency obtained is greater. If we consider the other average \( M'_2(\Pi_3) = M_{2,0}(\Pi_3) \times \frac{7}{8} + \frac{1}{8} \), then in the real case we obtain

<table>
<thead>
<tr>
<th>( N )</th>
<th>( M'_{2}(\Pi_3) )</th>
<th>( f_{\exp} )</th>
<th>( \delta )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 10^6 )</td>
<td>0,50989</td>
<td>0,48094</td>
<td>0,05678</td>
</tr>
<tr>
<td>( 10^7 )</td>
<td>0,50989</td>
<td>0,49054</td>
<td>0,03794</td>
</tr>
<tr>
<td>( 10^8 )</td>
<td>0,50989</td>
<td>0,49697</td>
<td>0,02533</td>
</tr>
<tr>
<td>( 10^9 )</td>
<td>0,50809</td>
<td>0,50120</td>
<td>0,01704</td>
</tr>
</tbody>
</table>

We now make the computation without the case \( d \equiv 6 \mod 9 \).

<table>
<thead>
<tr>
<th>( N )</th>
<th>( M_{2,0}(\Pi_3) )</th>
<th>( f_{\exp} )</th>
<th>( \delta )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 10^6 )</td>
<td>0,43987</td>
<td>0,40679</td>
<td>0,07521</td>
</tr>
<tr>
<td>( 10^7 )</td>
<td>0,43987</td>
<td>0,41776</td>
<td>0,05027</td>
</tr>
<tr>
<td>( 10^8 )</td>
<td>0,43987</td>
<td>0,42511</td>
<td>0,03356</td>
</tr>
<tr>
<td>( 10^9 )</td>
<td>0,43987</td>
<td>0,42995</td>
<td>0,02257</td>
</tr>
</tbody>
</table>

It remains to study the 9-rank in the case where \( d \equiv 6 \mod 9 \), and to try and find density formulas for the 9-rank. Finally, the discrepancy in the case \( p = 2 \) is explained by genus theory. Indeed, if the discriminant is divided by enough primes, then the torsion is not trivial. This explains why the frequency tends to 1.
ACKNOWLEDGEMENTS

It is the authors pleasure to thank Bill Allombert for his help with PARI/GP computations, Christophe Delaunay for his relevant suggestions and the anonymous referees who have devoted their time to study the previous versions of this article and suggested many improvements.

REFERENCES


