SCIENCE CHINA
Mathematics

• ARTICLES •

https://doi.org/10.1007/s11425-021-1946-0

On abelian 2-ramification torsion modules of quadratic fields

Jianing Li[1], Yi Ouyang[2,†] & Yue Xu[2,*]

[1]*Research Center for Mathematics and Interdisciplinary Sciences, Shandong University, Qingdao* 266237*, China;*
[2]*CAS Wu Wen-Tsun Key Laboratory of Mathematics, University of Science and Technology of China, Hefei* 230026*, China*

*Email: lijn@sdu.edu.cn, yiouyang@ustc.edu.cn, wasx*250*@mail.ustc.edu.cn*

Received January 27, 2021; accepted January 19, 2022; published online May 11, 2022

Abstract For a number field F and a prime number p, the $\mathbb{Z}_p$-torsion module of the Galois group of the maximal abelian pro-p extension of F unramified outside p over F, denoted by $\mathcal{T}_p(F)$, is an important subject in abelian p-ramification theory. In this paper, we study the group $\mathcal{T}_2(F) = \mathcal{T}_2(m)$ of the quadratic field $F = \mathbb{Q}(\sqrt{m})$. Firstly, assuming $m > 0$, we prove an explicit 4-rank formula for quadratic fields that $\mathrm{rk}_4(\mathcal{T}_2(-m)) = \mathrm{rk}_2(\mathcal{T}_2(-m)) - \mathrm{rank}(R)$, where R is a certain explicitly described Rédei matrix over $\mathbb{F}_2$. Furthermore, using this formula, we obtain the 4-rank density formula of $\mathcal{T}_2$-groups of imaginary quadratic fields. Secondly, for l an odd prime, we obtain results about the 2-power divisibility of orders of $\mathcal{T}_2(\pm l)$ and $\mathcal{T}_2(\pm 2l)$, both of which are cyclic 2-groups. In particular, we find that $\#\mathcal{T}_2(l) \equiv 2\#\mathcal{T}_2(2l) \equiv h_2(-2l) \pmod{16}$ if $l \equiv 7 \pmod 8$, where $h_2(-2l)$ is the 2-class number of $\mathbb{Q}(\sqrt{-2l})$. We then obtain density results for $\mathcal{T}_2(\pm l)$ and $\mathcal{T}_2(\pm 2l)$ when the orders are small. Finally, based on our density results and numerical data, we propose distribution conjectures about $\mathcal{T}_p(F)$ when F varies over real or imaginary quadratic fields for any prime p, and about $\mathcal{T}_2(\pm l)$ and $\mathcal{T}_2(\pm 2l)$ when l varies, in the spirit of Cohen-Lenstra heuristics. Our conjecture in the $\mathcal{T}_2(l)$ case is closely connected to Shanks-Sime-Washington's speculation on the distributions of the zeros of 2-adic L-functions and to the distributions of the fundamental units.

Keywords quadratic fields, density theorems, abelian 2-ramification

MSC(2020) 11R45, 11R11, 11R37

Citation: Li J N, Ouyang Y, Xu Y. On abelian 2-ramification torsion modules of quadratic fields. Sci China Math, 2022, 65, https://doi.org/10.1007/s11425-021-1946-0

1 Introduction

Let p be a prime number. For a number field F, let $M = M(F, p)$ be the maximal abelian pro-p extension of F unramified outside p. By the class field theory, $\mathrm{Gal}(M/F)$ is a finitely generated $\mathbb{Z}_p$-module of rank $r_2(F) + \delta_p(F) + 1$, where $r_2(F)$ is the number of complex places of F and $\delta_p(F) \geqslant 0$ is the Leopoldt defect of F at p. Leopoldt's conjecture is that $\delta_p(F) = 0$ for all p and F and this has been proved when $F/\mathbb{Q}$ is abelian. We call the $\mathbb{Z}_p$-torsion subgroup of $\mathrm{Gal}(M/F)$, a finite abelian p-group, the $\mathcal{T}_p$-group of F and denote it by $\mathcal{T}_p(F)$. The study of $\mathrm{Gal}(M/F)$ and $\mathcal{T}_p(F)$ which goes back to fundamental contributions

† Current address: Hefei National Laboratory, Hefei 230088, China
* Corresponding author

of Serre, Shafarevich and Brumer (see [8]), is the so-called abelian p-ramification theory. We refer the reader to the historical survey by Gras [8] for this theory, in which the p-rank formula for $\mathcal{T}_p(F)$ due to himself is stated. When F is totally real, by assuming $\delta_p(F)=0$, the work of Coates [2] and Colmez [3] shows that the order of $\mathcal{T}_p(F)$ is essentially the residue of the p-adic zeta function of F up to a p-adic unit. This motivates us to study the group structure of $\mathcal{T}_p(F)$ in more detail. Like class groups, the study of $\mathcal{T}_p(F)$ can be much more explicit in the case where F is a quadratic field and $p=2$. In this paper, we mainly consider this case, and our main purpose is to study the distribution of $\mathcal{T}_2(F)$ when F varies in a certain family of quadratic fields.

Note that the structure of a finite abelian p-group A is completely determined by its p^i-rank

$$\mathrm{rk}_{p^i}(A) := \dim_{\mathbb{F}_p} p^{i-1}A/p^iA$$

for all i. As a consequence, to study $\mathcal{T}_p(F)$, it is necessary and sufficient to study $\mathrm{rk}_{p^i}(\mathcal{T}_p(F))$ for all i.

The general p-rank formula for $\mathcal{T}_p(F)$ becomes very explicit for $p=2$ and F quadratic, after a computation of genus class numbers (see Theorem 2.1). If F is imaginary quadratic, we shall prove that an explicit 4-rank formula of $\mathcal{T}_2(F)$, namely, $\mathrm{rk}_4(\mathcal{T}_2(F))$ is the difference of $\mathrm{rk}_2(\mathcal{T}_2(F))$ and the rank of a certain explicitly described Rédei matrix (see Theorem 2.4). This formula is new and is analogous to the classical 4-rank formula for narrow class groups of quadratic fields. Applying this result, we deduce the following 4-rank density formula for $\mathcal{T}_2$-groups of imaginary quadratic fields, which is the main result of this paper.

Theorem 1.1 (4-rank density formula for $\mathcal{T}_2$ of imaginary quadratic fields)**.** *For integers $t\geqslant 1$ and $r\geqslant 0$, and a real number $x>0$, put*

$$\begin{aligned}
&N_x := \{m\in\mathbb{Z}_{>0} \mid m\leqslant x \text{ squarefree}\},\\
&N_{t;x} := \{m\in N_x \mid \text{exactly } t \text{ prime numbers are ramified in } \mathbb{Q}(\sqrt{-m})\},\\
&T^r_{t;x} := \{m\in N_{t;x} \mid \mathrm{rk}_4(\mathcal{T}_2(\mathbb{Q}(\sqrt{-m})))=r\}.
\end{aligned}$$

Then for any integer $r\geqslant 0$, the limit $d^T_{\infty,r}$, which is defined by

$$d^T_{\infty,r} := \lim_{t\to\infty}\lim_{x\to\infty}\frac{\#T^r_{t;x}}{\#N_{t;x}} \tag{1.1}$$

exists and

$$d^T_{\infty,r} = \frac{\prod_{i=r+2}^{\infty}(1-2^{-i})}{2^{r(r+1)}\prod_{i=1}^{r}(1-2^{-i})} = \frac{\eta_\infty(2)}{2^{r(r+1)}\eta_r(2)\eta_{r+1}(2)}, \tag{1.2}$$

where $\eta_s(q) := \prod_{i=1}^{s}(1-q^{-i})$ for $s\in\mathbb{Z}_{>0}\cup\{\infty\}$ and $q\geqslant 2$ and $\eta_0(q):=1$.

Remark 1.2. Theorem 1.1 is analogue to the density theorem of Gerth [5] on the 4-rank of narrow class groups of quadratic fields, and to the theorem of Yue and Yu [24] on the 4-rank of the tame kernel of quadratic fields.

We then turn to study the $\mathcal{T}_2$-groups of subfamilies of quadratic fields, namely, $\mathbb{Q}(\sqrt{\pm l})$ and $\mathbb{Q}(\sqrt{\pm 2l})$ where l is an odd prime. For simplicity, write $\mathcal{T}_2(m)$ for $\mathcal{T}_2(\mathbb{Q}(\sqrt{m}))$, $t_2(m)$ for its order and $h_2(m)$ for the 2-class number of $\mathbb{Q}(\sqrt{m})$. Such questions for $\mathcal{T}_2(l)$ and $\mathcal{T}_2(2l)$ have been studied by many researchers before. For example, consider $\mathbb{Q}(\sqrt{l})$ and let $L_2(1,\chi_l)$ be the 2-adic L-function, where χ_l is the quadratic character associated with $\mathbb{Q}(\sqrt{l})$. By recalling that $h_2(l)=1$, then Coates' order formula (see [2, Appendix 1] or Proposition 3.3) directly relates $\#\mathcal{T}_2(l)$ to the 2-adic regulator of $\mathbb{Q}(\sqrt{l})$ and therefore to the 2-adic valuation of $L_2(1,\chi_l)$ by the class number formula. The latter two objects and their relation to $h_2(-l)$ and $h_2(-2l)$ have been studied by Kaplan and Williams [10], Leonard and Williams [13], Williams [23] and Shanks et al. [19]. However, it seems that there is no study for $\mathcal{T}_2(-l)$ and $\mathcal{T}_2(-2l)$ before.

By the 2-rank formula (2.7), $\mathcal{T}_2(\pm l)=\mathcal{T}_2(\pm 2l)=0$ if $l\equiv\pm 3 \pmod 8$ and $\mathcal{T}_2(\pm l)$ and $\mathcal{T}_2(\pm 2l)$ are nontrivial 2-cyclic groups if $l\equiv\pm 1 \pmod 8$. Applying our 4-rank formula and Coates' order formula for totally real fields, we obtain the following results:

• (Theorem 3.1) Determine the congruent conditions for l satisfying $t_2(-l)$ or $t_2(-2l)$ equal to 2, 4 and greater than or equal to 8, and hence find the respective densities;

• (Theorem 3.7) Determine the conditions for $l \equiv 7 \pmod 8$ satisfying $t_2(l)$ equal to $4, 8$ and greater than or equal to 16, and deduce the formula

$$t_2(l) \equiv 2t_2(2l) \equiv h_2(-2l) \pmod{16}. \tag{1.3}$$

• (Proposition 3.9) Determine the conditions for $l \equiv 1 \pmod 8$ satisfying $t_2(l)$ or $t_2(2l)$ equal to 2 or 4.

Here, Theorem 3.1 is new, Theorem 3.7 is an improvement of the result in [13] and Proposition 3.9 is essentially a summary of the results in [10, 13, 23] by using the language of $\mathcal{T}_2$-groups.

For the real case, we then have the following density result which is inspired by the work on the distribution of 2-adic valuation of $L_2(1, \chi_l)$ in [19].

Theorem 1.3. *For $i \in \{0, 1\}$ and $e \in \{0, 1\}$,*

$$\lim_{x\to\infty} \frac{\#\{l \leqslant x : l \equiv (-1)^e \pmod 8, t_2(l) = 2^{i+1+e}\}}{\#\{l \leqslant x : l \equiv (-1)^e \pmod 8\}} = \frac{1}{2^{i+1}}, \tag{1.4}$$

$$\lim_{x\to\infty} \frac{\#\{l \leqslant x : l \equiv (-1)^e \pmod 8, t_2(2l) = 2^{i+1}\}}{\#\{l \leqslant x : l \equiv (-1)^e \pmod 8\}} = \frac{1}{2^{i+1}}. \tag{1.5}$$

In the last section, we shall present several conjectures in light of the density results we proved in the spirit of Cohen-Lenstra heuristics. We shall present the computational evidence for our conjectures in Appendixes A and B.

2 The rank and density formulas for quadratic imaginary fields

2.1 Notations

We shall use the following notations.

(1) For a general number field F, $\mathcal{O}_F$ is the ring of integers of F, $\mathcal{O}_F^\times$ is the group of units of F, r_1 and r_2 are respectively the numbers of real and complex places of F, and $n = r_1 + 2r_2 = [F : \mathbb{Q}]$. For a finite place v of F, we let U_v and $U_{1,v}$ be the groups of local units and principal local units, respectively. For v infinite, let $U_v = F_v^\times$. Let $\mathbb{A}_F$ be the adèle ring of F. The idèlic group of F, as the units of $\mathbb{A}_F$, is denoted by $\mathbb{A}_F^\times$.

Let

$$F^+ = \{\alpha \in F \mid v(\alpha) > 0 \text{ for all real places } v \text{ of } F\}$$

be the subgroup of $F^\times$ of totally real elements. Hence, $F^\times/F^+$ is an $\mathbb{F}_2$-vector space of dimension r_1, by the approximation theorem.

Let $S = S_p$ be the set of primes of F lying above p. Let $\mathcal{O}_S, E_S, \mathrm{Cl}_S$ and Cl_S^+ denote the ring of S-integers, the group of S-units, the S-class group and the narrow S-class group of F, respectively. Let $E_S^+ = E_S \cap F^+$ and $U_{1,S} = \prod_{v\in S} U_{1,v}$.

(2) In the special case where F is a quadratic field, write $F = \mathbb{Q}(\sqrt{m})$, and then (r_1, r_2) equals $(2, 0)$ if $m > 0$ and equals $(0, 1)$ if $m < 0$. Let $G = \mathrm{Gal}(F/\mathbb{Q}) = \{1, \sigma\}$. Let $\mathrm{Cl}(m)$, $\mathrm{Cl}_p(m)$, $h(m)$, $h_p(m)$ and $\mathcal{T}_p(m)$ be the class group, the p-class group, the class number, the p-class number and the $\mathcal{T}_p$-group of $F = \mathbb{Q}(\sqrt{m})$, respectively. Let $t_p(m) = \#\mathcal{T}_p(m)$.

If $p = 2$, the size of S is 2 if 2 splits and 1 if 2 is not split in F. If F is imaginary, $F^+ = F^\times$ and σ is the restriction of complex conjugation on F.

(3) For any abelian group A, $A[n]$ is the n-torsion subgroup of A and $A[p^\infty]$ is the p-primary part of A. For a finite abelian group A and a positive integer i, the p^i-rank $\mathrm{rk}_{p^i}(A) := \dim_{\mathbb{F}_p} p^{i-1}A/p^iA$. If A is an $\mathbb{F}_2$-vector space, $\dim A := \dim_{\mathbb{F}_2} A$ is its dimension.

(4) For Jacobi, 2nd Hilbert and Artin symbols with values in $\mu_2 = \{1, -1\}$, we use $[\cdot]$ instead of $(\cdot)$ to represent the corresponding additive symbols with values in $\mathbb{F}_2 = \{0, 1\}$.

2.2 The 2-rank and 4-rank formulas in general

For F a general number field, we recall some facts about $\mathcal{T}_p(F)$, all of which are standard consequences of the global class field theory (see, for example, [22, Theorem 13.4]). The closed subgroup $\overline{F^\times \prod_{v\notin S} U_v}$ of $\mathbb{A}_F^\times$ corresponds to the maximal abelian extension of F unramified outside S. Set

$$\mathcal{A}_F := \mathbb{A}_F^\times \Big/ \overline{F^\times \prod_{v\notin S} U_v}. \tag{2.1}$$

As it was shown in the proof of [22, Theorem 13.4], the induced Artin map $\mathcal{A}_F \twoheadrightarrow \mathrm{Gal}(M/F)$ is surjective and has finite kernel of prime-to-p order, and thus it induces a canonical isomorphism

$$\mathcal{A}_F^{\text{pro-}p} \cong \mathrm{Gal}(M/F),$$

where $\mathcal{A}_F^{\text{pro-}p}$ is the pro-p-part of $\mathcal{A}_F$. Let H be the p-Hilbert class field of F. Then $\mathrm{Gal}(H/F) \cong \mathrm{Cl}_p(F)$ canonically. Let ϕ be the canonical diagonal embedding $F \hookrightarrow \prod_{v\in S} F_v$ and $E_{1,S} = \phi^{-1}(U_{1,S}) \cap \mathcal{O}_F^\times$. By the class field theory, the following diagram is commutative with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & U_{1,S}/\overline{\phi(E_{1,S})} \arrow[r] \arrow[d, "\cong"] & \mathcal{A}_F^{\text{pro-}p} \arrow[r] \arrow[d, "\cong"] & \mathrm{Cl}_p(F) \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & \mathrm{Gal}(M/H) \arrow[r] & \mathrm{Gal}(M/F) \arrow[r] & \mathrm{Gal}(H/F) \arrow[r] & 0.
\end{tikzcd} \tag{2.2}$$

The group $U_{1,S}$ is a finitely generated $\mathbb{Z}_p$-module of rank $n = r_1 + 2r_2$ and the submodule $\overline{\phi(E_{1,S})}$ is of rank $r_1 + r_2 - 1 - \delta_p(F)$ for some integer $\delta_p(F) \geqslant 0$. It follows that $\mathrm{Gal}(M/F)$ is a finitely generated $\mathbb{Z}_p$-module of rank $r_2 + 1 + \delta_p(F)$. Leopoldt (see [22, Theorem 5.25]) conjectured that $\delta_p(F)$ is always 0 and this has been proved when F is abelian over $\mathbb{Q}$. Thus $\mathcal{T}_p(F)$, by definition the torsion subgroup of $\mathrm{Gal}(M/F)$, is finite and

$$\mathcal{T}_p(F) \cong \mathcal{A}_F[p^\infty], \tag{2.3}$$

and the p-rank of $\mathcal{T}_p(F)$ is given by

$$\mathrm{rk}_p(\mathcal{T}_p(F)) = \mathrm{rk}_p(\mathrm{Gal}(M/F)) - r_2 - 1 - \delta_p(F). \tag{2.4}$$

From now on, we identify $\mathcal{A}_F[p^\infty]$ with $\mathcal{T}_p(F)$. By abuse of notation, we write $\mathcal{A}_F$ and $\mathrm{Gal}(M/F)$ additively. Let L be the maximal abelian extension of F which is of exponent p and unramified outside p. Then L is the intermediate field of M/F fixed by $p\mathrm{Gal}(M/F)$. The induced Artin map

$$\mathcal{A}_F \to \mathrm{Gal}(M/F)$$

has the kernel consisting of prime-to-p-torsion elements, and hence is contained in $p\mathcal{A}_F$ and the induced map

$$\mathcal{A}_F/p\mathcal{A}_F \to \mathrm{Gal}(L/F)$$

is an isomorphism. The kernel of the composite map

$$\varphi : \mathcal{T}_p(F)[p] \hookrightarrow \mathcal{A}_F \to \mathcal{A}_F/p\mathcal{A}_F = \mathrm{Gal}(L/F)$$

is

$$\mathcal{T}_p(F)[p] \cap p\mathcal{A}_F = p\mathcal{T}_p(F)[p^2],$$

which is an $\mathbb{F}_p$-space of dimension $\mathrm{rk}_{p^2}(\mathcal{T}_p(F))$. This gives the identity

$$\mathrm{rk}_{p^2}(\mathcal{T}_p(F)) = \mathrm{rk}_p(\mathcal{T}_p(F)) - \dim_{\mathbb{F}_p} \mathrm{Im}(\varphi). \tag{2.5}$$

We first derive the 2- and 4-rank formulas of $\mathcal{T}_2$ for a general number field, and then obtain the 2-rank formula for a quadratic field. The general 2-rank formula (2.6) below was proved in [6, Théorème I 3], and the 4-rank formula is quite routine.

Theorem 2.1. *Let F be a number field, S be the set of primes in F above 2 and Cl_S^+ be the narrow S-class group of F.*

(1) (*See* [6]) *The 2-rank of $\mathcal{T}_2(F)$ is given by the formula*

$$\mathrm{rk}_2\mathcal{T}_2(F) = \#S + \mathrm{rk}_2(\mathrm{Cl}_S^+) - 1 - \delta_2(F). \tag{2.6}$$

In particular, if m is a squarefree integer with t odd prime factors, then for $F = \mathbb{Q}(\sqrt{m})$,

$$\mathrm{rk}_2(\mathcal{T}_2(F)) = \begin{cases} t, & \text{if } q \equiv \pm 1 \pmod 8 \text{ for all odd prime } q \mid m, \\ t-1, & \text{if } q \equiv \pm 3 \pmod 8 \text{ for some odd prime } q \mid m. \end{cases} \tag{2.7}$$

(2) *Suppose that A is a finite set of idèles which generates*

$$\mathcal{T}_2(F) \subset \mathcal{A}_F := \mathbb{A}_F^\times \Big/ \overline{F^\times \prod_{v \nmid 2} U_v}.$$

Suppose that B is a finite set of elements in $F^\times$ such that $F(\sqrt{B})$ is the maximal abelian extension of F of exponent 2 unramified outside 2. For $a \in A$ and $b \in B$, let

$$[a, b] = \log_{-1}(a, F(\sqrt{b})) \in \mathbb{F}_2$$

be the additive Artin symbol. Let $R = ([a, b])_{a\in A, b\in B}$. Then

$$\mathrm{rk}_4(\mathcal{T}_2(F)) = \mathrm{rk}_2(\mathcal{T}_2(F)) - \mathrm{rank}(R). \tag{2.8}$$

Remark 2.2. (1) The minimal size of A is $\mathrm{rk}_2(\mathcal{T}_2(F))$, and the minimal size of B is

$$\mathrm{rk}_2(\mathrm{Gal}(M/F)) = \mathrm{rk}_2(\mathcal{T}_2(F)) + r_2(F) + 1 + \delta_2(F).$$

Moreover, if $F(\sqrt{b})$ is contained in a $\mathbb{Z}_2$-extension of F, then $[a, b] = 0$ for all $a \in A$ and we can delete the corresponding row in R.

(2) The p^2-rank formula for $\mathcal{T}_p(F)$ in the case $\mu_p \subseteq F$ can be proved similarly, as the kernel of the map

$$\mathcal{T}_p(F)[p] \hookrightarrow \mathcal{A}_F \to \mathcal{A}_F/p\mathcal{A}_F \cong \mathrm{Gal}(L/F)$$

is $p\mathcal{T}_p[p^2]$. Moreover, one can similarly deduce the formula

$$\mathrm{rk}_{p^{i+1}}(\mathcal{T}_p(F)) = \mathrm{rk}_{p^i}(\mathcal{T}_p(F)) - \dim_{\mathbb{F}_p} \mathrm{Im}(\mathcal{T}_p(F)[p^i] \to \mathrm{Gal}(L/K)).$$

Proof of Theorem 2.1. We are in the case $p = 2$. Then L is the maximal abelian extension of F of exponent 2 unramified outside S. By Kummer theory, $L = F(\sqrt{J})$, where J is the finite subgroup of $F^\times/F^{\times 2}$ given by

$$J := \{\beta \in F^+ \mid \beta\mathcal{O}_S = \mathfrak{b}^2 \text{ for some } \mathcal{O}_S\text{-fractional ideal } \mathfrak{b} \text{ of } F\}/(F^\times)^2. \tag{2.9}$$

(1) First, suppose that F is general. The non-degeneracy of the Kummer pairing $J \times \mathrm{Gal}(L/F) \to \{\pm 1\}$ then implies

$$\mathrm{rk}_2\mathrm{Gal}(M/F) = \dim \mathrm{Gal}(L/F) = \dim J. \tag{2.10}$$

Let pr be the natural projection $\mathrm{Cl}_S^+ \to \mathrm{Cl}_S$ and $\mathrm{Cl}_{S,+} = \mathrm{pr}(\mathrm{Cl}_S^+[2]) \subset \mathrm{Cl}_S[2]$. For $[\beta] \in J$ and $\beta\mathcal{O}_S = \mathfrak{b}^2$, then the class map $\mathrm{cl}_S(\mathfrak{b})$ lies in $\mathrm{Cl}_{S,+}$. This gives an exact sequence of $\mathbb{F}_2$-vector spaces, i.e.,

$$1 \to E_S^+/E_S^2 \to J \xrightarrow{\beta \mapsto \mathrm{cl}_S(\mathfrak{b})} \mathrm{Cl}_{S,+} \to 1. \tag{2.11}$$

Let $F^\times\mathcal{O}_S = \{\alpha\mathcal{O}_S \mid \alpha \in F^\times\}$ and $F^+\mathcal{O}_S = \{\alpha\mathcal{O}_S \mid \alpha \in F^+\}$. Then $\ker \mathrm{pr} = F^\times\mathcal{O}_S/F^+\mathcal{O}_S \subset \mathrm{Cl}_S^+[2]$. This gives an exact sequence of $\mathbb{F}_2$-vector spaces

$$1 \to F^\times\mathcal{O}_S/F^+\mathcal{O}_S \to \mathrm{Cl}_S^+[2] \to \mathrm{Cl}_{S,+} \to 1. \tag{2.12}$$

We also have the following natural exact sequence of $\mathbb{F}_2$-vector spaces:

$$1 \to E_S/E_S^+ \to F^\times/F^+ \to F^\times\mathcal{O}_S/F^+\mathcal{O}_S \to 1. \tag{2.13}$$

Combining the above results, we get

$$\begin{aligned}\mathrm{rk}_2\mathrm{Gal}(M/F) &= \dim E_S^+/E_S^2 + \dim \mathrm{Cl}_{S,+}\\ &= \dim E_S^+/E_S^2 + \dim \mathrm{Cl}_S^+[2] - r_1 + \dim E_S/E_S^+\\ &= \dim E_S/E_S^2 + \dim \mathrm{Cl}_S^+[2] - r_1\\ &= r_2 + \#S + \dim \mathrm{Cl}_S^+[2],\end{aligned}$$

where $\dim F^\times/F^+ = r_1$ by the approximation theorem, and $\dim E_S/E_S^2 = r_1 + r_2 + \#S$ by Dirichlet's unit theorem that $E_S \cong \mathbb{Z}^{r_1+r_2+\#S-1} \times \mathbb{Z}/d\mathbb{Z}$ with d even. By (2.4), we then get the general 2-rank formula (2.6) for $\mathcal{T}_2$-group of a general base field (see [6] for a slightly different approach).

Now suppose that $F = \mathbb{Q}(\sqrt{m})$ is a quadratic field. Then $\delta_2(F) = 0$. Write $G = \mathrm{Gal}(F/\mathbb{Q})$. Since $\mathbb{Q}$ has class number 1, we conclude that $\mathrm{Cl}_S^+[2] = (\mathrm{Cl}_S^+)^G$. Recall that t is the number of odd prime factors of m. Applying the S-narrow version of the ambiguous class number formula (see, for example, [16, Remark 4.5]) gives the following result:

$$\dim(\mathrm{Cl}_S^+)^G = \begin{cases} t-2, & \text{if 2 splits and } 2 \notin N(F),\\ t-1, & \text{if 2 splits and } 2 \in N(F) \text{ or 2 does not split and } 2 \notin N(F),\\ t, & \text{if 2 does not split and } 2 \in N(F).\end{cases} \tag{2.14}$$

By Lemma 2.3 below, $2 \in N(F)$ if and only if $q \equiv \pm 1 \pmod 8$ for all the odd primes $q \mid m$, and then the 2-rank formula (2.7) for $F = \mathbb{Q}(\sqrt{m})$ follows.

(2) We may assume that $\widetilde{B} = \{b \pmod{F^{\times 2}} \mid b \in B\}$ is an $\mathbb{F}_2$-basis of J. Then

$$\mathrm{Gal}(L/F) \hookrightarrow \prod_{b\in B} \mathrm{Gal}(F(\sqrt{b})/F)$$

is an isomorphism. Written additively, the map φ sends $a \in \mathcal{T}_2(F)[2] \subset \mathcal{A}_F$ to $([a, F(\sqrt{b})])_{b\in B}$. Thus $\dim_{\mathbb{F}_2}(\mathrm{Im}(\varphi))$ is nothing but the rank of $([a,b])_{a\in A, b\in B}$. By (2.5), we get the 4-rank formula. □

We have the following easy lemma to transform the norm conditions into congruent conditions.

Lemma 2.3. *Let m be a positive squarefree integer, $F = \mathbb{Q}(\sqrt{-m})$ and $\widetilde{F} = \mathbb{Q}(\sqrt{m})$. Then*

$$\begin{aligned}&2 \in N(F) \Leftrightarrow 2 \in N(\widetilde{F}) \Leftrightarrow q \equiv \pm 1 \pmod 8 \textit{ for all odd prime } q \mid m,\\ &-2 \in N(\widetilde{F}) \Leftrightarrow q \equiv 1,\, 3 \pmod 8 \textit{ for all odd prime } q \mid m,\\ &-1 \in N(\widetilde{F}) \Leftrightarrow q \equiv 1 \pmod 4 \textit{ for all odd prime } q \mid m.\end{aligned}$$

Proof. By Hasse's norm theorem and the product formula, $2 \in N(F)$ if and only if $2 \in N(F_v)$ for all but one prime v of F. If $v \nmid 2m$, then v is always unramified and $2 \in N(F_v)$ by local class field theory. For an odd prime $q \mid m$, q is ramified in F. Let $\mathfrak{q}$ be the unique ramified prime of F above q. Then $2 \in N(F_\mathfrak{q})$ if and only if the Hilbert symbol $(2, -m)_q = 1$, which is equivalent to that $q \equiv \pm 1 \pmod 8$. If 2 splits in F, then $v \mid 2$ is unramified and $2 \in N(F_v)$; in other cases, there is only one prime v above 2 which can be excluded from consideration. Hence, $2 \in N(F)$ if and only if $q \equiv \pm 1 \pmod 8$ for every odd prime $q \mid m$. The other cases can be proved similarly. □

2.3 The explicit 4-rank formula for imaginary quadratic fields

We turn to work on the imaginary quadratic field case. We shall work out A and B explicitly for an imaginary quadratic field and hence obtain an explicit 4-rank formula in this case. This explicit formula will be used to deduce the 4-rank density formula of $\mathcal{T}_2$-groups of imaginary quadratic fields in the next subsection.

We suppose $m>0$ and $F=\mathbb{Q}(\sqrt{-m})$. Let $\{q_1,\dots,q_t\}$ be the set of odd prime factors of m, arranged in such a way that $q_i\equiv\pm1 \pmod 8$ if $1\leqslant i\leqslant k$ and $\pm3 \pmod 8$ if $k<i\leqslant t$. Note that $k=0$ if $q\equiv\pm3 \pmod 8$ for all $q\mid m$. Let $\mathfrak{p}$ be a prime of F above 2. Then $\mathfrak{p}$ is either the unique prime above 2 or $(2)=\mathfrak{p}\bar{\mathfrak{p}}$ splits in F, where $\bar{\mathfrak{p}}\neq\mathfrak{p}$ is the complex conjugate of $\mathfrak{p}$. Let $\mathfrak{q}_i$ be the unique prime of F above q_i. For an odd prime q, let $q^*=(-1)^{(q-1)/2}q$. Then q_i^* $(1\leqslant i\leqslant k)$ and $q_j^*q_{j'}^*$ $(k<j,j'\leqslant t)$ are squares in the 2-adic field $\mathbb{Q}_2$.

Our explicit 4-rank formula for $\mathcal{T}_2(\mathbb{Q}(\sqrt{-m}))$ is the following theorem.

Theorem 2.4. *Suppose $F=\mathbb{Q}(\sqrt{-m})$. For $0\leqslant i\leqslant t$, we define the idèles $a_i=(a_{i,v})\in\mathbb{A}_F^\times$ as follows:*

(1) $a_{0,\mathfrak{p}}=\sqrt{-1}$ if $F_\mathfrak{p}\cong\mathbb{Q}_2(\sqrt{-1})$, and $a_{0,\mathfrak{p}}=-1$ if $(2)=\mathfrak{p}\bar{\mathfrak{p}}$ splits in F;

(2) if $1\leqslant i\leqslant k$, $a_{i,\mathfrak{q}_i}=\sqrt{-m}$ and $a_{i,v}=\sqrt{q_i^*}$ for $v\mid 2$;

(3) if $k<i<t$, $a_{i,\mathfrak{q}_i}=a_{i,\mathfrak{q}_t}=\sqrt{-m}$ and $a_{i,v}=\sqrt{q_i^*q_t^*}$ for $v\mid 2$;

(4) for all other places v, $a_{i,v}=1$. In particular, $a_t=1$ if $k<t$.

Let π be a generator of $\mathfrak{p}^\lambda$, where λ is the order of $\mathfrak{p}$ in the class group of F. If 2 is a norm of F, noting that m is a norm of $\mathbb{Z}[\sqrt{2}]$, write $m=2g^2-h^2$ with $g,h\in\mathbb{Z}_{>0}$ and define

$$\alpha=\begin{cases} h+\sqrt{-m}, & \text{if } 2\in N(F)\setminus N\left(\left(\mathcal{O}_F\left[\frac{1}{2}\right]\right)^\times\right),\\ 1, & \text{otherwise}.\end{cases}\tag{2.15}$$

Let

$$A=\{a_0,\dots,a_t\}\subset\mathbb{A}_F^\times,\quad B=\{-1,q_1,\dots,q_t,\pi,\alpha\}\subset F^\times.\tag{2.16}$$

Then A and $B\cup\{2\}$ satisfy the assumptions in Theorem 2.1(2)*, and $[a,2]=0$ for $a\in A$. Hence,*

$$\mathrm{rk}_4(\mathcal{T}_2(F))=\mathrm{rk}_2(\mathcal{T}_2(F))-\mathrm{rank}(R),\quad \textit{where } R=([a,b])_{a\in A,b\in B}.\tag{2.17}$$

Remark 2.5. For F a general real quadratic field, it is still quite easy to find B, but the harder part is to find a set of generators A for $\mathcal{T}_2(F)[2]$. One reason is that it is not known how to obtain a system of explicit generators $\mathrm{Cl}(F)[2]$ for an arbitrary real quadratic field F by a general formula.

If $t=1$, then $F=\mathbb{Q}(\sqrt{-1})$ or $F=\mathbb{Q}(\sqrt{-2})$. In this case, Theorem 2.4 can be verified directly. We shall assume $t>1$ in what follows. For an ideal $\mathfrak{a}$ of F, let $\mathrm{cl}(\mathfrak{a})$ be its ideal class in $\mathrm{Cl}(F)$, and $\mathrm{cl}_S(\mathfrak{a})$ be its class in the S-class group Cl_S of F.

Theorem 2.4 is then a consequence of the following three propositions.

Proposition 2.6. *Let L be the maximal abelian extension of exponent* 2 *over F, unramified outside S. Then $L=F(\sqrt{B'})$, where $B'=B\cup\{2\}=\{-1,2,q_1,\dots,q_t,\pi,\alpha\}$.*

Proof. We include the proof, which is routine, for lack of exact references. Let J' be the subgroup of $F^\times/(F^\times)^2$ generated by B'. It suffices to show that $J'=J$ with J defined in (2.9).

We note that for all $x\in B'$ and $x\neq\alpha$, $F(\sqrt{x})/F$ is unramified outside S. Thus if one can show that $F(\sqrt{\alpha})/F$ is unramified outside S, then $J'\subseteq J$.

Suppose first that either $2\in N(E_S)$ or $2\notin N(F)$. In this case, $\alpha=1$ and hence $J'\subset J$. We shall use the exact sequence (2.11) to show that J' is indeed equal to J. Since F is imaginary, $F^+=F^\times$. (2.11) becomes the following exact sequence:

$$1\to E_S/E_S^2\to J\xrightarrow{g}\mathrm{Cl}_S[2]\to 1.\tag{2.18}$$

Here, we recall that the map g sends β to $\mathrm{cl}_S(\mathfrak{b})$, for $\beta\in J$ satisfying $\beta\mathcal{O}_S=\mathfrak{b}^2$ for some $\mathcal{O}_S$-fractional ideal $\mathfrak{b}$. Clearly, $E_S/E_S^2\subset J'$, as E_S is generated by $-1,2$ and π. Thus, in order to prove $J'=J$, it suffices to show that $g(J')=\mathrm{Cl}_S[2]$. Let $G=\mathrm{Gal}(F/\mathbb{Q})$. Then $\mathrm{Cl}_S^G=\mathrm{Cl}_S[2]$. Let I_S be the subgroup of fractional ideals of F which is generated by prime ideals not in S. There is an isomorphism (see [16, Section 4])

$$\mathrm{Coker}(I_S^G\to\mathrm{Cl}_S^G)\cong\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)^\times\cap N(F^\times)/N(E_S).\tag{2.19}$$

Since $-1 \notin N(F)$ as F is imaginary, the assumption that either $2 \in N(E_S)$ or $2 \notin N(F^\times)$ precisely implies that the group on the right-hand side of (2.19) is trivial. Thus Cl_S^G is generated by I_S^G. But I_S^G is generated by the ramified primes (see [16, Lemma 4.4]), it follows that $\mathrm{Cl}_S^G = \langle \mathfrak{q}_1, \ldots, \mathfrak{q}_t \rangle$. Since $g(q_i) = \mathrm{cl}_S(\mathfrak{q}_i)$ for each i, this proves $g(J') = \mathrm{Cl}_S^G = \mathrm{Cl}_S[2]$. Therefore, we have $J' = J$ when either $2 \in N(E_S)$ or $2 \notin N(F)$.

Suppose next that $2 \in N(F)$ but $2 \notin N(E_S)$. By Lemma 2.3, $q_i \equiv \pm 1 \pmod 8$ for $1 \leqslant i \leqslant t$. Hence we can write $m = 2g^2 - h^2$ for some $g, h \in \mathbb{Z}_{>0}$. In this case, $\alpha = h + \sqrt{-m}$ (see (2.15)). Then $\alpha + \bar{\alpha} = 2h$ and $\alpha\bar{\alpha} = 2g^2$, where $\bar{\alpha}$ is the complex conjugate of α. Clearly, $\gcd(g, h) = 1$. It follows that $\gcd((\alpha), (\bar{\alpha})) \mid 2\mathcal{O}_F$.

(1) If $m \equiv 1 \pmod 8$ or $2 \mid m$, then $2\mathcal{O}_F = \mathfrak{p}^2$ is ramified in F and g is odd. In this case, $\mathfrak{p} \mid (\alpha)$ but $2 \nmid (\alpha)$, otherwise $4 \mid \alpha\bar{\alpha} = 2g^2$. Hence $\bar{\mathfrak{p}} = \mathfrak{p} \mid (\bar{\alpha})$ and $\gcd((\alpha), (\bar{\alpha})) = \mathfrak{p}$. Since the integral ideals $(\alpha)\mathfrak{p}^{-1}$ and $(\bar{\alpha})\mathfrak{p}^{-1}$ are coprime to each other and their product is a square, and hence there exists an $\mathcal{O}_F$-integral ideal $\mathfrak{a}$ such that $(\alpha) = \mathfrak{p}\mathfrak{a}^2$.

(2) If $m \equiv 7 \pmod 8$, then $2\mathcal{O}_F = \mathfrak{p}\bar{\mathfrak{p}}$ splits and g is even. Without loss of generality, we may assume $\mathfrak{p} \mid \alpha$. Then $\bar{\mathfrak{p}} \mid \bar{\alpha}$ and hence $\bar{\mathfrak{p}} \mid \alpha = 2h - \bar{\alpha}$. This means $2 \mid \alpha$ and $\gcd((\alpha), (\bar{\alpha})) = 2\mathcal{O}_F$. Now $\frac{\alpha}{2} \cdot \frac{\bar{\alpha}}{2} = 2 \cdot (\frac{g}{2})^2$, and then one and only one of $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ divides $\frac{\alpha}{2}$. Assume $\mathfrak{p} \mid \frac{\alpha}{2}$. Then the two integral ideals $(\alpha/2)\mathfrak{p}^{-1}$ and $(\bar{\alpha}/2)\bar{\mathfrak{p}}^{-1}$ are coprime and their product is a square, and hence there exists an $\mathcal{O}_F$-integral ideal $\mathfrak{a}$ such that $(\alpha) = 2\mathfrak{p}\mathfrak{a}^2$.

Thus, in both cases, we have

$$\alpha\mathcal{O}_S = \mathfrak{a}^2\mathcal{O}_S. \tag{2.20}$$

This shows that $F(\sqrt{\alpha})/F$ is unramified outside S. Hence $J' \subset J$. Following the same argument in the previous case and applying (2.18), to show $J' = J$, we just need to show $g(J') = \mathrm{Cl}_S[2] = \mathrm{Cl}_S^G$. If we can prove $\mathrm{Cl}_S^G = \langle \mathrm{cl}_S(I_S^G), \mathrm{cl}_S(\mathfrak{a}) \rangle$, by the facts that $\mathrm{cl}_S(I_S^G) \subset g(J')$ and $\mathrm{cl}_S(\mathfrak{a}) = g(\alpha) \in g(J')$, then we are done.

We are left to prove the claim $\mathrm{Cl}_S^G = \langle \mathrm{cl}_S(I_S^G), \mathrm{cl}_S(\mathfrak{a}) \rangle$. By the isomorphism (2.19) and by our assumption $2 \in N(F) \setminus N(E_S)$, we have $[\mathrm{Cl}_S^G : \mathrm{cl}_S(I_S^G)] = 2$. Thus we just need to show $\mathrm{cl}_S(\mathfrak{a}) \notin \mathrm{cl}_S(I_S^G)$. Suppose, on the contrary, $\mathrm{cl}_S(\mathfrak{a}) \in \mathrm{cl}_S(I_S^G)$. Then we have $\mathrm{cl}(\mathfrak{a}) \in \langle \mathrm{cl}(I_S^G), \mathrm{cl}(\mathfrak{p}), \mathrm{cl}(\bar{\mathfrak{p}}) \rangle$, since by definition, $\mathrm{Cl}_S = \mathrm{Cl}_F / \langle \mathrm{cl}(S) \rangle$. Also note that $\mathrm{cl}(\bar{\mathfrak{p}}) = \mathrm{cl}(\mathfrak{p})^{-1}$. So we can write $\mathrm{cl}(\mathfrak{a}) = \mathrm{cl}(\mathfrak{p})^{r_0} \prod_i \mathrm{cl}(\mathfrak{q}_i)^{r_i}$ for some integers $r_i \in \mathbb{Z}$. Then $\mathrm{cl}(\mathfrak{a})^2 = \mathrm{cl}(\mathfrak{p})^{2r_0}$. But we have shown that $\mathrm{cl}(\mathfrak{a})^2 = \mathrm{cl}(\mathfrak{p})^{-1}$. Hence $\mathfrak{p}^{2r_0+1}$ would be principal, say $\mathfrak{p}^{2r_0+1} = (\gamma)$. This implies that $2 = N(\gamma/2^{r_0}) \in N(E_S)$, which contradicts our assumption that $2 \in N(F^\times) \setminus N(E_S)$. This proves the claim. □

Lemma 2.7. *If $m \equiv 3 \pmod 4$, then $\{\mathrm{cl}(\mathfrak{q}_1), \ldots, \mathrm{cl}(\mathfrak{q}_{t-1})\}$ is a basis of the $\mathbb{F}_2$-vector space $\mathrm{Cl}(F)[2]$. If $m \equiv 1 \pmod 4$, then $\{\mathrm{cl}(\mathfrak{p}), \mathrm{cl}(\mathfrak{q}_1), \ldots, \mathrm{cl}(\mathfrak{q}_{t-1})\}$ is a basis of $\mathrm{Cl}(F)[2]$. If $m \equiv 2 \pmod 4$, then $\{\mathrm{cl}(\mathfrak{q}_1), \ldots, \mathrm{cl}(\mathfrak{q}_t)\}$ is a basis of $\mathrm{Cl}(F)[2]$.*

Proof. The proof is the classical genus theory and we refer to [4, Theorem 6.1] for the details. □

Proposition 2.8. *Let $\hat{A}$ be the image of A in $\mathcal{A}_F$. Then $\mathcal{T}_2(F)[2] = \hat{A}$.*

Proof. For each i, a_i^2 is clearly in $\overline{F^\times \prod_{v \notin S} U_v}$, and hence $\hat{a}_i$, the image of a_i in $\mathcal{A}_F$, is in $\mathcal{A}_F[2] = \mathcal{T}_2(F)[2]$, and $\hat{A} \subseteq \mathcal{T}_2(F)[2]$. We have the following exact sequence of $\mathbb{F}_2$-vector spaces induced from (2.2):

$$0 \to U_{1,S}/\overline{\phi(E_{1,S})}[2] \to \mathcal{T}_2(F)[2] \xrightarrow{f} \mathrm{Cl}(F)[2]. \tag{2.21}$$

Since $E_{1,S} = \{\pm 1\}$, the first term of (2.21) has order 2 and is generated by $\hat{a}_0$ if $F_\mathfrak{p} = \mathbb{Q}_2$ or $\mathbb{Q}_2(\sqrt{-1})$, and is trivial otherwise. Thus $\dim \mathrm{Ker}(f) = \dim \mathrm{Ker}(f\,|_{\hat{A}}) = 1$ if $F_\mathfrak{p} = \mathbb{Q}_2$ or $\mathbb{Q}_2(\sqrt{-1})$, and 0 otherwise. By definition, $f(\hat{a}_i) = \mathrm{cl}(\mathfrak{q}_i)$ if $1 \leqslant i \leqslant k$ and $f(\hat{a}_j) = \mathrm{cl}(\mathfrak{q}_j)\mathrm{cl}(\mathfrak{q}_t)$ if $k < j < t$.

Suppose first that $m \equiv 2 \pmod 4$. In this case, $F_\mathfrak{p}$ cannot be $\mathbb{Q}_2$ or $\mathbb{Q}_2(\sqrt{-1})$, so $\mathrm{Ker}(f) = 0$ and $\dim(\hat{A}) = \dim f(\hat{A})$. If $t = k$, then $\dim f(\hat{A}) = t$ by Lemma 2.7. Then $\mathcal{T}_2(F)[2] = \hat{A}$ by the 2-rank formula (2.7) for $\mathcal{T}_2(F)$. If $t > k$, one can write

$$(f(\hat{a}_1), \ldots, f(\hat{a}_k), f(\hat{a}_{k+1}\hat{a}_t), \ldots, f(\hat{a}_{t-1}\hat{a}_t)) = (\mathrm{cl}(\mathfrak{q}_1), \ldots, \mathrm{cl}(\mathfrak{q}_t))M,$$

where M is a matrix of rank $t-1$. Note that $\{\mathrm{cl}(\mathfrak{q}_1),\dots,\mathrm{cl}(\mathfrak{q}_t)\}$ is an $\mathbb{F}_2$-basis of $\mathrm{Cl}(F)[2]$ by Lemma 2.7, and then $\dim\hat{A}=\dim f(\hat{A})=\mathrm{rank}(M)=t-1$. However, $\dim\mathcal{T}_2(F)[2]=t-1$ by (2.7) if $t>k$, and hence $\mathcal{T}_2(F)[2]=\hat{A}$.

Suppose next that $m\equiv\pm1 \pmod 8$. Then $t-k$ is even and $F_{\mathfrak{p}}=\mathbb{Q}_2$ or $\mathbb{Q}_2(\sqrt{-1})$. If $t=k$, it follows from Lemma 2.7 that $\dim f(\hat{A})=t-1$ and hence $\dim\hat{A}=t$ which coincides with $\dim\mathcal{T}_2(F)[2]$ by (2.7). If $t-k$ is positive and even, this time we can write

$$(f(\hat{a}_1),\dots,f(\hat{a}_k),f(\hat{a}_{k+1}\hat{a}_t),\dots,f(\hat{a}_{t-1}\hat{a}_t))=(\mathrm{cl}(\mathfrak{q}_1),\dots,\mathrm{cl}(\mathfrak{q}_{t-1}))M,$$

where M is a matrix of rank $t-2$. Note that $\{\mathrm{cl}(\mathfrak{q}_1),\dots,\mathrm{cl}(\mathfrak{q}_{t-1})\}$ is linearly independent by Lemma 2.7, and then $\dim\hat{A}=\dim f(\hat{A})+1=\mathrm{rank}(M)+1=t-1$, which coincides with $\dim\mathcal{T}_2(F)[2]$ by the 2-rank formula (2.7). This proves $\mathcal{T}_2(F)[2]=\hat{A}$ when $m\equiv\pm1 \pmod 8$.

Finally, suppose that $m\equiv\pm3 \pmod 8$. It follows that $t-k$ is an odd integer and the local field $F_{\mathfrak{p}}$ cannot be $\mathbb{Q}_2$ or $\mathbb{Q}_2(\sqrt{-1})$. Then

$$(f(\hat{a}_1),\dots,f(\hat{a}_k),f(\hat{a}_{k+1}\hat{a}_t),\dots,f(\hat{a}_{t-1}\hat{a}_t))=(\mathrm{cl}(\mathfrak{q}_1),\dots,\mathrm{cl}(\mathfrak{q}_{t-1}))M,$$

where M is a matrix of rank $t-1$. Thus $\dim\hat{A}=\dim f(\hat{A})=t-1$, which coincides with $\dim\mathcal{T}_2(F)[2]$ by the 2-rank formula (2.7). This proves $\mathcal{T}_2(F)[2]=\hat{A}$ when $m\equiv\pm3 \pmod 8$. □

Proposition 2.9. *$[a,2]=0$ for all $a\in A$.*

Proof. Since $F(\sqrt{2})$ is the first layer of the cyclotomic $\mathbb{Z}_2$-extension of F, the proposition then follows from Remark 2.2(1). □

2.4 4-rank density formula

The aim of this subsection is to prove Theorem 1.1. We first give a simplification of the matrix R in Theorem 2.4 when 2 is not a norm of $F=\mathbb{Q}(\sqrt{-m})$. Although only the result in the case $m\equiv3 \pmod 4$ will be used in the proof of Theorem 1.1, we also present the simplification in the case $m\equiv1,2 \pmod 4$ for completeness.

Theorem 2.10. *Let $F=\mathbb{Q}(\sqrt{-m})$, where m is a positive squarefree integer. Let $q_1,q_2,\dots,q_t$ be all the ramified prime numbers in F and assume that $q_1=2$ if 2 is ramified in F. Set*

$$R^C:=\left(\left[\frac{q_i,-m}{q_j}\right]\right)_{2\leqslant i,j\leqslant t}\in M_{t-1}(\mathbb{F}_2)$$

and

$$\tau:=\begin{cases}\left(\left[\frac{-2}{q_2}\right],\dots,\left[\frac{-2}{q_t}\right]\right)^{\mathrm{T}}, & \textit{if } m\equiv3 \ (\mathrm{mod}\ 8),\\ \left(\left[\frac{2}{q_2}\right],\dots,\left[\frac{2}{q_t}\right]\right)^{\mathrm{T}}, & \textit{otherwise.}\end{cases}$$

If $2\notin N(F)$, then

$$\mathrm{rk}_4\mathcal{T}_2(F)=t-1-\mathrm{rank}(\tau,R^C). \tag{2.22}$$

Remark 2.11. A word on the notation: note that in the above theorem, $q_1,\dots,q_t$ denote the ramified primes in F rather than the odd prime factors of m as used in Theorem 2.4 and in last subsection. Clearly, this makes no difference when $m\equiv3 \pmod 4$.

Remark 2.12. Recall that (see, for example, [16, Section 2]) the classical Rédei matrix for Cl_F is

$$R^{\mathrm{Cl}}:=\left(\left[\frac{q_i,-m}{q_j}\right]\right)_{1\leqslant i,j\leqslant t}\quad\text{and}\quad \mathrm{rk}_4(\mathrm{Cl}_F)=t-1-\mathrm{rank}R^{\mathrm{Cl}}.$$

The matrix R^C defined above is obtained from R^{Cl} by deleting its first row and first column. When $m\equiv2,3 \pmod 4$, using the quadratic reciprocity law, one sees that the sums of each row and of each column of R^{Cl} are zero, and hence $\mathrm{rank}R^C=\mathrm{rank}R^{\mathrm{Cl}}$. Therefore,

$$\mathrm{rk}_4\mathrm{Cl}_F=t-1-\mathrm{rank}R^C,\quad \text{if } m\equiv2,3 \ (\mathrm{mod}\ 4).$$

Proof of Theorem 2.10. Firstly, we consider the case where 2 is unramified, i.e., $m \equiv 3 \pmod 4$. Then $\mathrm{rk}_2(\mathcal{T}_2(F)) = t-1$ by Theorem 2.1.

(1) First assume $m \equiv 3 \pmod 8$. Then 2 is inert in F. Note that

$$\sum_{i=1}^{t} \left[\frac{-2}{q_i}\right] = \left[\frac{-2}{m}\right] = 0. \tag{2.23}$$

Hence, we can rearrange $\{q_1, \ldots, q_t\}$ without changing the rank of (τ, R^C). In this case, the sets A and B of Theorem 2.4 are as follows: $a_0 = a_t = 1$, $\alpha = 1$ and $\pi = 2$. But by Proposition 2.9, $[a, 2] = 0$ for each $a \in A$. So we may assume that $A = \{a_1, \ldots, a_{t-1}\}$ and $B = \{-1 := q_0, q_1, \ldots, q_t\}$. Clearly, B can be replaced by $\{-1 := q_0^*, q_1^*, \ldots, q_t^*\}$ as they generate the same group.

For $1 \leqslant i \leqslant t$, note that $\sqrt{q_i^*} \in F_{\mathfrak{p}} = \mathbb{Q}_2(\sqrt{5})$ and define

$$a_i' := \Big(\ldots, \underset{\mathfrak{p}}{\sqrt{q_i^*}}, \ldots, \underset{\mathfrak{q}_i}{\sqrt{-m}}, \ldots\Big) \in \mathbb{A}_F^{\times}.$$

Then we have $a_i = a_i'$ for $1 \leqslant i \leqslant k$ and $a_j = a_j' a_t'$ for $k < j \leqslant t-1$. Since $m \equiv 3 \pmod 8$, $t-k$ must be odd. Then a direct computation shows

$$a_1 \cdots a_{t-1} \equiv a_t' \left(\mathrm{mod}\ \left(\mathbb{A}_F^{\times 2}, \overline{F^\times \prod_{v \notin S} U_v}\right)\right).$$

It follows that we may replace A by $\{a_1', \ldots, a_t'\}$ as they generate the same group in $\mathcal{T}_2(F)$. Therefore, by Theorem 2.4, we have

$$\mathrm{rk}_4 \mathcal{T}_2(F) = t - 1 - \mathrm{rank}([a_i', q_j^*])_{1 \leqslant i \leqslant t, 0 \leqslant j \leqslant t}.$$

Using the quadratic reciprocity law, for $i, j \geqslant 1$, one checks that

$$[a_i', -1] = \left[\frac{-2}{q_i}\right] \quad \text{and} \quad [a_i',\ q_j^*] = \left[\frac{m, q_j^*}{q_i}\right] = \left[\frac{q_i, -m}{q_j}\right].$$

By the row-sum-zero and column-sum-zero property of the matrix mentioned in Remark 2.12 and the equation (2.23), we conclude that

$$\mathrm{rk}_4 \mathcal{T}_2(F) = t - 1 - \mathrm{rank}(\tau, R^C).$$

(2) Then assume $m \equiv 7 \pmod 8$. The prime 2 splits in F. Note that $t > k$ since $2 \notin N(F)$, and hence the element $a_t \in A$ is trivial. We still replace B by $\{-1 := q_0, \pi, q_1^*, \ldots, q_t^*\}$. Also note that both $a_0 \in A$ and $\pi \in B$ are nontrivial. We may choose the sign of π such that $[\frac{\pi, -1}{\mathfrak{p}}] = 0$. Then $[a_0, \pi] = 0$. The matrix R for $\mathcal{T}_2(F)$ in Theorem 2.4 is

$$R = \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots \\ [\frac{-1}{q_1}] & [\frac{\sqrt{-m}, \pi}{\mathfrak{q}_1}] & \cdots & [\frac{m, q_j^*}{q_1}] & \cdots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ [\frac{-1}{q_t q_{k+1}}] & [\frac{\sqrt{-m}, \pi}{\mathfrak{q}_{k+1}}] + [\frac{\sqrt{-m}, \pi}{\mathfrak{q}_t}] & \cdots & [\frac{m, q_j^*}{q_{k+1}}] + [\frac{m, q_j^*}{q_t}] & \cdots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ [\frac{-1}{q_t q_{t-1}}] & [\frac{\sqrt{-m}, \pi}{\mathfrak{q}_{t-1}}] + [\frac{\sqrt{-m}, \pi}{\mathfrak{q}_t}] & \cdots & [\frac{m, q_j^*}{q_{t-1}}] + [\frac{m, q_j^*}{q_t}] & \cdots \end{pmatrix}. \tag{2.24}$$

We make the following elementary operations on the matrix R: firstly, replace the first column by $(1, 0, \ldots, 0)^{\mathrm{T}}$, and replace the first row $(\cdots)$ by $(1, [\frac{\sqrt{-m}, \pi}{\mathfrak{q}_t}], \ldots, [\frac{m, q_j^*}{q_t}], \ldots)$. Secondly, add the first row to the $(k+2)$-th, $(k+3)$-th, $\ldots$, t-th rows. Thirdly, move the first row to the bottom. Finally, delete the first row. It follows that the matrix R in (2.24) is equivalent to

$$(\tau, \beta, R^C), \tag{2.25}$$

where

$$\beta := \left(\left[\frac{\sqrt{-m},\pi}{\mathfrak{q}_i}\right]\right)^{\mathrm{T}}_{2\leqslant i\leqslant t}.$$

By Lemma 2.13 below, $\mathrm{rank}(R)=\mathrm{rank}(\tau,R^C)$. This proves the case $m\equiv 7 \pmod 8$ by Theorem 2.4.

Now we consider the case where 2 is ramified whence $q_1=2$. Then $m=q_2\cdots q_t\equiv 1 \pmod 4$ or $m=2q_2\cdots q_t\equiv 2 \pmod 4$. Write $2\mathcal{O}_F=\mathfrak{p}^2$. By our condition $2\notin N(F)$, B in Theorem 2.4 is $B=\{q_0^*:=-1,q_2^*,\ldots,q_t^*\}$.

(3) Suppose $m\equiv 1 \pmod 8$. Then $A=\{a_0,a_2,\ldots,a_{t-1}\}$. It is clear that the matrix R for $\mathcal{T}_2(F)$ is

$$R=\begin{pmatrix} 0 & \cdots & 0 & \cdots \\ 0 & \cdots & [\frac{m,q_j^*}{q_2}] & \cdots \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & [\frac{m,q_j^*}{q_{k+1}}]+[\frac{m,q_j^*}{q_t}] & \cdots \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & [\frac{m,q_j^*}{q_{t-1}}]+[\frac{m,q_j^*}{q_t}] & \cdots \end{pmatrix}$$

Firstly, replace the first row $(\cdots)$ by $(1,\ldots,[\frac{m,q_j^*}{q_t}],\ldots)$. Then we get a matrix whose rank equals $1+\mathrm{rank}R$. Secondly, add the first row to the $(k+2)$-th, $(k+3)$-th, $\ldots$, t-th rows. Finally, move the first row to the bottom. Now we get (τ,R^C). We have $\mathrm{rk}_2\,\mathcal{T}_2(F)=t-2$ by Theorem 2.1. Thus,

$$\mathrm{rk}_4\mathcal{T}_2(-m)=t-2-\mathrm{rank}R=t-1-\mathrm{rank}(\tau,R^C).$$

This proves the case $m\equiv 1 \pmod 8$. The arguments for the other cases are similar and we leave the details to the reader. □

Lemma 2.13. *Assume that* $m\equiv 7 \pmod 8$ *having a prime factor* $q\equiv \pm 3 \pmod 8$. *Then* β *is a sum of column vectors of* R^C.

Proof. Let λ be the order of $\mathfrak{p}$ in $\mathrm{Cl}(F)$. Suppose that $\pi=\frac{c+d\sqrt{-m}}{2}$ with $c,d\in\mathbb{Z}$ such that $\pi\mathcal{O}_F=\mathfrak{p}^\lambda$ and $(\frac{-1,\pi}{\mathfrak{p}})=1$. Note that λ must be even; otherwise, $2=N(\pi 2^{-\frac{\lambda-1}{2}})\in N(F)$ which contradicts the assumption. Write $\lambda=2\lambda'$. Then we have a decomposition in $\mathbb{Z}$:

$$(2^{\lambda'+1}-c)(2^{\lambda'+1}+c)=md^2. \tag{2.26}$$

Since $(\frac{-1,\pi}{\mathfrak{p}})=1$, it follows from the product formula that $(\frac{-1,\pi}{\bar{\mathfrak{p}}})=1$. We obtain $\pi\equiv 1 \pmod{\bar{\mathfrak{p}}^2}$ and $\bar{\pi}\equiv 1 \pmod{\mathfrak{p}^2}$. But $\mathfrak{p}^\lambda\mid\pi$ and λ is even, we have $\pi\equiv 0 \pmod{\mathfrak{p}^2}$. Thus

$$c=\pi+\bar{\pi}\equiv 1 \pmod{\mathfrak{p}}^2 \Rightarrow c\equiv 1 \pmod 4.$$

Then $2^{\lambda'+1}-c$ and $2^{\lambda'+1}+c$ are coprime, and by (2.26), there exist positive integers m_+, m_-, d_+ and d_- such that $m=m_+m_-$, $d=d_+d_-$, $2^{\lambda'+1}+c=m_+d_+^2$ and $2^{\lambda'+1}-c=m_-d_-^2$. In particular, $m_+\equiv c\equiv 1 \pmod 4$ and $m_-\equiv -1 \pmod 4$. We obtain

$$2c=m_+d_+^2-m_-d_-^2.$$

Now the vector

$$\beta=\left(\left[\frac{q_i,2c}{q_i}\right]\right)^{\mathrm{T}}_{1\leqslant i\leqslant t}.$$

If $q_i\mid m_-$, noting that $m_+\equiv 1 \pmod 4$, we have

$$\left[\frac{q_i,2c}{q_i}\right]=\left[\frac{q_i,m_+}{q_i}\right]=\sum_{q\mid 2m_+}\left[\frac{q_i,m_+}{q}\right]=\sum_{q\mid m_+}\left[\frac{q_i,m_+}{q}\right]=\sum_{q\mid m_+}\left[\frac{q_i,-m}{q}\right].$$

If $q_i \mid m_+$, noting that $-m_- \equiv 1 \pmod 4$, we also have

$$\left[\frac{q_i, 2c}{q_i}\right] = \left[\frac{q_i, -m_-}{q_i}\right] = \sum_{q \mid 2m_-} \left[\frac{q_i, -m_-}{q}\right] = \sum_{q \mid m_-} \left[\frac{q_i, -m_-}{q}\right] = \sum_{q \mid m_-} \left[\frac{q_i, -m}{q}\right] = \sum_{q \mid m_+} \left[\frac{q_i, -m}{q}\right].$$

This means that β is the sum of the column vectors $([\frac{q_i, -m}{q_j}])_i^{\mathrm{T}}$ for $q_j \mid m_+$ of R^C. □

The rest of this subsection is dedicated to proving Theorem 1.1, which is based on the work of Gerth [5] and Yue and Yu [24]. As in the statement of Theorem 1.1, x will always denote a positive real number and t will denote a positive integer.

The set $N_{t,x}$ is the disjoint union of subsets $N_{t,x}^{(i)}$ $(i = 1, 2, 3)$ defined by (all p_i's are odd distinct primes)

$$\begin{aligned} N_{t,x}^{(1)} &:= \{m \in N_{t,x} \mid m = p_1 \cdots p_t \equiv 3 \pmod 4\}, \\ N_{t,x}^{(2)} &:= \{m \in N_{t,x} \mid m = p_1 \cdots p_{t-1} \equiv 1 \pmod 4\}, \\ N_{t,x}^{(3)} &:= \{m \in N_{t,x} \mid m = 2p_1 \cdots p_{t-1} \equiv 2 \pmod 4\}. \end{aligned}$$

Following [5], we know that when $x \to \infty$,

$$\begin{aligned} \#N_{t;x}^{(1)} &\sim \frac{1}{2} \frac{1}{(t-1)!} \frac{x(\log\log x)^{t-1}}{\log x}, \\ \#N_{t;x}^{(2)} &\sim \frac{1}{2} \frac{1}{(t-2)!} \frac{x(\log\log x)^{t-2}}{\log x} = o(\#N_{t;x}^{(1)}), \\ \#N_{t;x}^{(3)} &\sim \frac{1}{(t-2)!} \frac{x(\log\log(x/2))^{t-2}}{2\log(x/2)} = o(\#N_{t;x}^{(1)}). \end{aligned}$$

Here and after we define $f(x) \sim g(x)$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$ and $f(x) = o(g(x))$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$. Then

$$\#N_{t;x} \sim \#N_{t;x}^{(1)} \sim \frac{1}{2} \frac{1}{(t-1)!} \frac{x(\log\log x)^{t-1}}{\log x}. \tag{2.27}$$

We define two equivalence relations in $N_{t,x}^{(1)}$.

Definition 2.14. For $m = p_1 \cdots p_t$ and $n = q_1 \cdots q_t \in N_{t,x}^{(1)}$ which are arranged such that $p_1 < p_2 < \cdots < p_t$ and $q_1 < q_2 < \cdots < q_t$, we say that m and n have the same Rédei type if $q_i \equiv p_i \pmod 4$ for $i \leqslant t$ and $[\frac{q_j}{q_i}] = [\frac{p_j}{p_i}]$ for $1 \leqslant j < i \leqslant t$; we say that m and n have the same Rédei type modulo 8, if furthermore $q_i \equiv p_i \pmod 8$ for $i \leqslant t$. Denote by $[m]$ (resp. $[[m]]$) the equivalence class of m with the same Rédei type (resp. modulo 8), respectively.

Lemma 2.15. *For any $m \in N_{t,x}^{(1)}$, we define*

$$\begin{aligned} R(m; t, x) &:= [m] \cap N_{t,x}^{(1)} = \{m' \in N_{t,x}^{(1)} \mid m' \textit{ and } m \textit{ have the same Rédei type}\}, \\ S(m; t, x) &:= [[m]] \cap N_{t,x}^{(1)} = \{m' \in N_{t,x}^{(1)} \mid m' \textit{ and } m \textit{ have the same Rédei type modulo } 8\}. \end{aligned}$$

Then when $x \to \infty$, we have

$$\#R(m; t, x) \sim 2^{1-\frac{t^2+t}{2}} \cdot \#N_{t,x}^{(1)}$$

and

$$\#S(m; t, x) \sim \frac{\#R(m; t, x)}{2^t}.$$

Proof. See [24, Lemma 2.1 and Corollary 2.2]. □

Remark 2.16. As mentioned in [5, p. 493], an intuitive explanation of the above lemma might proceed as follows. To decide the equivalence class $[m]$, we need to fix the conditions $p_i \pmod 4$ for $l \leqslant i \leqslant t-1$ since $m = \prod_{i=1}^t p_i \equiv 3 \pmod 4$, and the conditions $[\frac{p_j}{p_i}]$ for $1 \leqslant j < i \leqslant t$. Hence, there are $2^{\frac{t^2+t}{2}-1}$

equivalence classes and the proportion of each equivalence class in $N_{t,x}^{(1)}$ is the same by the above lemma. Furthermore, given a class $[m]$, then $\{p_1 \pmod 8, \ldots, p_t \pmod 8\}$ have 2^t choices. Hence, there are 2^t modulo 8 equivalence classes in $[m]$ and the proportion of each modulo 8 equivalence class in $[m]$ is the same by the above lemma again.

Lemma 2.17. *Let $W(t,x) = \{m \in N_{t,x}^{(1)} \mid 2 \in N(\mathbb{Q}(\sqrt{-m}))\}$. Then*

$$\lim_{t\to\infty}\lim_{x\to\infty} \frac{\#W(t,x)}{\#N_{t,x}^{(1)}} = 0.$$

Proof. Put

$$f(m) = \begin{cases} 1, & \text{if } 2 \in N(\mathbb{Q}(\sqrt{-m})), \\ 0, & \text{otherwise.} \end{cases}$$

Given an equivalence class $[m]$, we claim that there is exactly one class $[[n]]$ in $[m]$ such that $f(n) = 1$. Indeed, $q_i \pmod 4$ is determined as $n = q_1 \cdots q_t \in [m]$. Then by Hasse's norm theorem, $f(n) = 1$ implies that q_i must be $1 \pmod 8$ (resp. $7 \pmod 8$) in $1 \pmod 4$ (resp. $3 \pmod 4$). Hence the claim follows.

Now we have

$$\begin{aligned} \lim_{t\to\infty}\lim_{x\to\infty} \frac{\#W(t,x)}{\#N_{t,x}^{(1)}} &= \lim_{t\to\infty}\lim_{x\to\infty} \frac{\sum_{[m]} \sum_{[[n]],n\in[m]} f(n)\cdot \#S(n;t,x)}{\sum_{[m]} \sum_{[[n]],n\in[m]} \#S(n;t,x)} \\ &= \lim_{t\to\infty}\lim_{x\to\infty} \frac{\sum_{[m]} \#R(m;t,x)/2^t}{\sum_{[m]} \#R(m;t,x)} \\ &= \lim_{t\to\infty} \frac{1}{2^t} = 0, \end{aligned}$$

where the second equality is by Lemma 2.15. □

Proof of Theorem 1.1. By Theorem 2.10, Lemma 2.17 and the estimate (2.27), it suffices to prove that for $r \geqslant 0$,

$$\lim_{t\to\infty}\lim_{x\to\infty} \frac{\#\{m \in N_{t,x}^{(1)} \mid \mathrm{rank}(\tau, R^C) = t-1-r\}}{\#N_{t;x}^{(1)}} = \frac{\eta_\infty(2)}{2^{r(r+1)}\eta_r(2)\eta_{r+1}(2)}.$$

For any matrix $A \in M_{t-1}(\mathbb{F}_2)$, write $\mathrm{Im}A := \{Ax \mid x \in \mathbb{F}_2^{t-1}\}$. Then we only need to prove that

$$\lim_{t\to\infty}\lim_{x\to\infty} \frac{\#\{m \in N_{t,x}^{(1)} \mid \mathrm{rank}R^C = t-1-r, \tau \in \mathrm{Im}R^C\}}{\#N_{t;x}^{(1)}} = \frac{1}{2^r}\cdot\frac{\eta_\infty(2)}{2^{r^2}\eta_r(2)^2} \tag{2.28}$$

and

$$\lim_{t\to\infty}\lim_{x\to\infty} \frac{\#\{m \in N_{t,x}^{(1)} \mid \mathrm{rank}R^{\mathrm{Cl}} = t-2-r, \tau \notin \mathrm{Im}R^{\mathrm{Cl}}\}}{\#N_{t;x}^{(1)}} = \left(1 - \frac{1}{2^{r+1}}\right)\cdot\frac{\eta_\infty(2)}{2^{(r+1)^2}\eta_{r+1}(2)^2}, \tag{2.29}$$

since

$$\frac{1}{2^r}\cdot\frac{\eta_\infty(2)}{2^{r^2}\eta_r(2)^2} + \left(1 - \frac{1}{2^{r+1}}\right)\cdot\frac{\eta_\infty(2)}{2^{(r+1)^2}\eta_{r+1}(2)^2} = \frac{\eta_\infty(2)}{2^{r(r+1)}\eta_r(2)\eta_{r+1}(2)}.$$

By Lemma 2.15 and [24, Remark 2.3, Equation (3.19)], in each equivalence class $[m] \subset N_{t,x}^{(1)}$, $\tau \in \mathrm{Im}R^C$ has probability $\frac{2^{t-1-r}}{2^{t-1}} = \frac{1}{2^r}$ if $\mathrm{rank}R^C = t-1-r$, i.e.,

$$\lim_{t\to\infty}\lim_{x\to\infty} \frac{\#\{m \in N_{t,x}^{(1)} \mid \mathrm{rank}R^C = t-1-r, \tau \in \mathrm{Im}R^C\}}{\#\{m \in N_{t,x}^{(1)} \mid \mathrm{rank}R^C = t-1-r\}} = \frac{1}{2^r}.$$

It is proved by Gerth [5] that

$$\lim_{t\to\infty}\lim_{x\to\infty} \frac{\#\{m \in N_{t,x}^{(1)} \mid \mathrm{rank}R^C = t-1-r\}}{\#N_{t;x}^{(1)}} = \frac{\eta_\infty(2)}{2^{r^2}\eta_r(2)^2}.$$

This implies the equation (2.28). The proof of the equation (2.29) is similar and we leave the details to the reader. Thus

$$d_{\infty,r}^T = \frac{1}{2^r}\cdot\frac{\eta_\infty(2)}{2^{r^2}\eta_r(2)^2} + \left(1-\frac{1}{2^{r+1}}\right)\cdot\frac{\eta_\infty(2)}{2^{(r+1)^2}\eta_{r+1}(2)^2} = \frac{\eta_\infty(2)}{2^{r(r+1)}\eta_r(2)\eta_{r+1}(2)}.$$

This completes the proof of Theorem 1.1. □

3 Study of $\mathcal{T}_2(\pm l)$ and $\mathcal{T}_2(\pm 2l)$ for odd prime l

By the 2-rank formula (2.7), if l is a prime, $\mathcal{T}_2(\pm l)$ and $\mathcal{T}_2(\pm 2l)$ are trivial if $l \equiv \pm 3 \pmod 8$, and nontrivial cyclic 2-groups if $l \equiv \pm 1 \pmod 8$. In what follows, we assume that $l \equiv \pm 1 \pmod 8$ is a prime. In this section, we study the structures of $\mathcal{T}_2(\pm l)$ and $\mathcal{T}_2(\pm 2l)$, or equivalently, the 2-power divisibility of their orders $t_2(\pm l)$ and $t_2(\pm 2l)$.

3.1 The imaginary case

Theorem 3.1. *Let $l \equiv \pm 1 \pmod 8$ be a prime. Then $\mathcal{T}_2(-l)$ and $\mathcal{T}_2(-2l)$ are nontrivial cyclic 2 groups, and*

(1) $t_2(-l) = 2$ *if* $l \equiv 7 \pmod 8$, $t_2(-l) = 4$ *if* $l \equiv 9 \pmod{16}$, *and* $t_2(-l) \geqslant 8$ *if* $l \equiv 1 \pmod{16}$;

(2) $t_2(-2l) = 2$ *if* $l \equiv 7 \pmod 8$ *or* $l \equiv 9 \pmod{16}$, *and* $t_2(-2l) \geqslant 4$ *if* $l \equiv 1 \pmod{16}$.

Remark 3.2. Based on the numerical data, we find out that the conditions $t_2(-l) = 2^i$ for $i \geqslant 3$ and $t_2(-2l) = 2^i$ for $i \geqslant 2$ are not classified by congruence relations.

Proof of Theorem 3.1. (1) Let $F = \mathbb{Q}(\sqrt{-l})$. We consider (i) $l \equiv 7 \pmod 8$ and (ii) $l \equiv 1 \pmod 8$ separately.

(i) In this case, $2 \nmid h(-l)$ by genus theory. From the commutative diagram (2.2), we have

$$\mathcal{T}_2(-l) \cong ((\mathbb{Z}_2^\times \times \mathbb{Z}_2^\times)/\pm 1)[2^\infty] \cong \mathbb{Z}/2\mathbb{Z}.$$

(ii) In this case, 2 is ramified and $F_\mathfrak{p} = \mathbb{Q}_2(\sqrt{-1})$.

Let

$$a = \Big(\dots, \underset{\mathfrak{p}}{1+\sqrt{-1}}, \dots\Big) \in \mathbb{A}_F^\times$$

and $\hat{a}$ be its image in $\mathcal{A}_F$; here, we recall that $\mathcal{A}_F$ is the group defined in (2.1) with $p = 2$. Then

$$a^4 = \Big(\dots, \underset{\mathfrak{p}}{-4}, \dots\Big) \in \overline{F^\times \prod_{v\notin S} U_v}$$

and hence, $\hat{a} \in \mathcal{T}_2(F)[4]$. Since

$$a^2 = \Big(\dots, \underset{\mathfrak{p}}{2\sqrt{-1}}, \dots\Big) \equiv \Big(\dots, \underset{\mathfrak{p}}{\sqrt{-1}}, \dots\Big) \bmod \Big(\overline{F^\times \prod_{v\notin S} U_v}\Big)$$

and $\sqrt{-1}$ is nontrivial in $U_{1,\mathfrak{p}}/\{\pm 1\} \subset \mathcal{A}_F^{\text{pro-}2}$, we have $\hat{a}^2 \neq 0$ in $\mathcal{T}_2(F)$. Thus $\hat{a}$ is a generator of the cyclic group $\mathcal{T}_2(F)[4]$.

The 2-units E_S of F is generated by -1 and 2. Clearly, $2 \notin N(E_S)$. Write $l = 2g^2 - h^2$. Let $\alpha = h + \sqrt{-l}$. By Proposition 2.6, $L = F(\sqrt{-1}, \sqrt{l}, \sqrt{2}, \sqrt{\alpha}) = F(\sqrt{-1}, \sqrt{2}, \sqrt{\alpha})$ is the maximal abelian extension of exponent 2 over F unramified outside 2. The map

$$\mathcal{T}_2(F)[4] \to \mathrm{Gal}(F(\sqrt{-1})/F) \times \mathrm{Gal}(F(\sqrt{2})/F) \times \mathrm{Gal}(F(\sqrt{\alpha})/F)$$

has kernel $2\mathcal{T}_2(F)[8]$. Thus $t_2(-l) \geqslant 8$ if and only if the additive Artin symbols $[a,-1]=[a,2]=[a,\alpha]=0$. It is easy to see that $[a,2]=[a,-1]=0$ since $l \equiv 1 \pmod 8$. We have

$$\begin{aligned}[a, h+\sqrt{-l}] &= \left[\frac{1+\sqrt{-1}, h+\sqrt{-l}}{F_{\mathfrak{p}}}\right] = \left[\frac{-\sqrt{l}, h+\sqrt{-l}}{F_{\mathfrak{p}}}\right] + \left[\frac{-\sqrt{l}-\sqrt{-l}, h+\sqrt{-l}}{F_{\mathfrak{p}}}\right]\\ &= \left[\frac{-\sqrt{l}, 2g^2}{\mathbb{Q}_2}\right] + \left[\frac{-\sqrt{l}-\sqrt{-l}, h+\sqrt{-l}}{F_{\mathfrak{p}}}\right]\\ &= \left[\frac{\sqrt{l}, 2}{\mathbb{Q}_2}\right] + \left[\frac{-\sqrt{l}-\sqrt{-l}, h+\sqrt{-l}}{F_{\mathfrak{p}}}\right].\end{aligned}$$

Note that

$$\left[\frac{\sqrt{l}, 2}{\mathbb{Q}_2}\right] = \begin{cases} 0, & \text{if } l \equiv 1 \pmod{16},\\ 1, & \text{if } l \equiv 9 \pmod{16}.\end{cases}$$

For any $x, y \in F_{\mathfrak{p}}$, noting that -1 is a square in $F_{\mathfrak{p}}$, we have

$$0 = \left[\frac{\frac{x}{x+y}, \frac{y}{x+y}}{F_{\mathfrak{p}}}\right] = \left[\frac{xy, x+y}{F_{\mathfrak{p}}}\right] + \left[\frac{x+y, x+y}{F_{\mathfrak{p}}}\right] + \left[\frac{x, y}{F_{\mathfrak{p}}}\right].$$

Put $x = -\sqrt{l}-\sqrt{-l}$ and $y = h+\sqrt{-l}$. Note that $x+y \in \mathbb{Q}_2$. It follows that $[\frac{x+y, x+y}{F_{\mathfrak{p}}}] = 0$. Thus,

$$\left[\frac{x, y}{F_{\mathfrak{p}}}\right] = \left[\frac{x+y, xy}{F_{\mathfrak{p}}}\right] = \left[\frac{x+y, 4g^2 l}{\mathbb{Q}_2}\right] = 0.$$

This proves (1).

(2) follows from the same argument used in the proof of (1). We omit the details here. □

3.2 The real case

We need the following order formula of Coates (see [2, Appendix] or [7, Chapter III.2.6.5]).

Proposition 3.3. *Let $K \neq \mathbb{Q}$ be a totally real number field. Assume that the Leopoldt Conjecture holds for (p, K), i.e., $\delta_p(K) = 0$. Then*

$$\#\mathcal{T}_p(K) = (p\text{-adic unit}) \cdot \frac{p \cdot [K \cap \mathbb{Q}^{p,\mathrm{cyc}} : \mathbb{Q}] \cdot h(K) \cdot R_p(K)}{\sqrt{D_K} \cdot \prod_{\mathfrak{p} \mid p} N\mathfrak{p}}. \tag{3.1}$$

Here, $h(K)$ is the class number, $R_p(K)$ is the p-adic regulator, D_K is the discriminant of K, $\mathbb{Q}^{p,\mathrm{cyc}}$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, the product runs over all the primes of K lying above p, and N is the norm map from K to $\mathbb{Q}$.

Lemma 3.4. *Assume that $l \equiv \pm 1 \pmod 8$ is a prime. Let ν_2 be the normalized 2-adic valuation and $\log_2$ be the 2-adic logarithmic map. For m equal to l or $2l$, let $\varepsilon_m = a_m + b_m\sqrt{m}$ be the fundamental unit of $\mathbb{Q}(\sqrt{m})$. Then*

(1) $\nu_2(t_2(l)) = \nu_2(\log_2(\varepsilon_l)) - 1 = \nu_2(a_l) - 1$;

(2) $\nu_2(t_2(2l)) = \nu_2(h(2l)) + \nu_2(b_{2l}) - 1$.

Proof. (1) Let $F = \mathbb{Q}(\sqrt{l})$. Recall that the 2-adic regulator $R_2(F)$ is $\log_2(\varepsilon_l)$. By Coates' order formula above, we have $\nu_2(t_2(l)) = \nu_2(\log_2(\varepsilon_l)) - 1$ as $2 \nmid h(l)$. It remains to show that $\nu_2(\log_2(\varepsilon_l)) = \nu_2(a_l)$. We use the basic property of logarithm that for $x \in \overline{\mathbb{Q}}_2$, if $\nu_2(x-1) > 1$, then $\nu_2(\log_2(x)) = \nu_2(x)$.

If $l \equiv 1 \pmod 8$, then it is easy to see that a_l and b_l are integers. It is also known that $N(\varepsilon_l) = a_l^2 - lb_l^2 = -1$. It follows that $4 \mid a_l$, and b_l is odd. Thus, $\nu_2(\varepsilon_l^2 - 1) = \nu_2(\varepsilon_l^2 + \varepsilon_l\bar{\varepsilon}_l) = 1 + \nu_2(a_l) \geqslant 3$. This implies that $\nu_2(\log_2(\varepsilon_l^2)) = \nu_2(\varepsilon_l^2 - 1) = 1 + \nu_2(a_l)$. Hence, $\nu_2(\log_2(\varepsilon_l)) = \nu_2(a_l)$.

If $l \equiv 7 \pmod 8$, we first prove that a_l is even. In this case, 2 is ramified in F, i.e., $2\mathcal{O}_F = \mathfrak{p}^2$. Since $h(l)$ is odd, $\mathfrak{p}$ must be principal, i.e., $\mathfrak{p} = (\pi)$ with $\pi \in \mathcal{O}_F$. Then $\pi^2/2$ is a unit, i.e., ε_l^k. Note that k must be odd. Otherwise, $\sqrt{2} \in F$, which is absurd. Then $(\pi\varepsilon_l^{-(k-1)/2})^2 = 2\varepsilon_l$ and hence $\pi\varepsilon_l^{-(k-1)/2} \in \mathcal{O}_F$. Write $\pi\varepsilon_l^{-(k-1)/2} = c + d\sqrt{l}$ with $c, d \in \mathbb{Z}$. Then c and d must be odd since $N(c + d\sqrt{l}) = 2$. Hence, $a_l = \frac{c^2+d^2l}{2}$ is clearly even.

Thus, b_l must be odd. Then $\nu_2(\varepsilon_l^4 - 1) = \nu_2(\varepsilon_l^4 - \varepsilon_l^2\bar{\varepsilon}_l^2) = 2 + \nu_2(a_l b_l) = 2 + \nu(a_l)$. Therefore, $\nu_2(\log_2(\varepsilon_l)) = \nu_2(a_l)$. This completes the proof of (1).

(2) Clearly, a_{2l} is odd and b_{2l} is even. We have

$$\nu_2(\varepsilon_{2l}^4 - 1) = \nu_2(\varepsilon_{2l}^2 + \varepsilon_{2l}\bar{\varepsilon}_{2l}) + \nu_2(\varepsilon_{2l}^2 - \varepsilon_{2l}\bar{\varepsilon}_{2l}) = \nu_2(2a_{2l}) + \nu_2(2\sqrt{2l}b_{2l}) = \frac{5}{2} + \nu_2(b_{2l}).$$

Hence, $\nu_2(\log_2(\varepsilon_{2l})) = \frac{1}{2} + \nu_2(b_{2l})$. Then (2) follows from Coates' order formula for $\mathcal{T}_2(\mathbb{Q}(\sqrt{2l}))$. □

Remark 3.5. The proof that a_l is even for $l \equiv 7 \pmod 8$ also holds for $l \equiv 3 \pmod 4$. For a different proof of this fact, see [25].

The following proposition collects results about the 2-class groups $\mathrm{Cl}_2(-l)$ and $\mathrm{Cl}_2(-2l)$ due to Gauss (see [4]), Hasse [9], Brown [1] and others, most importantly due to Leonard and Williams [13]; please see [15, Theorem 4.2] for a proof about $\mathrm{Cl}_2(-2l)$.

Proposition 3.6. *Let l be an odd prime. Then both $\mathrm{Cl}_2(-l)$ and $\mathrm{Cl}_2(-2l)$ are cyclic groups.*

(1) *$h_2(-l) = 1$ if $l \equiv 3 \pmod 4$, $h_2(-l) = 2$ if $l \equiv 5 \pmod 8$ and $h_2(-l) \geqslant 4$ if $l \equiv 1 \pmod 8$. Moreover, if $l \equiv 1 \pmod 8$, suppose $l = 2g^2 - h^2$, then $h_2(-l) = 4$ if and only if $g \equiv 3 \pmod 4$, and $h_2(-l) = 8$ if and only if $(\frac{2h}{g})(\frac{g}{l})_4 = -1$.*

(2) *$h_2(-2l) = 2$ if $l \equiv \pm 3 \pmod 8$ and $h_2(-2l) \geqslant 4$ if $l \equiv \pm 1 \pmod 8$. Moreover,*

(i) *if $l \equiv 1 \pmod 8$, suppose $l = u^2 - 2v^2$ such that $u \equiv 1 \pmod 4$, then $h_2(-2l) = 4$ if and only if $u \equiv 5 \pmod 8$, and $h_2(-2l) = 8$ if and only if $(\frac{u}{l})_4 = -1$;*

(ii) *if $l \equiv 7 \pmod 8$, then $h_2(-2l) = 4$ if and only if $l \equiv 7 \pmod{16}$, and $h_2(-2l) = 8$ if and only if $l \equiv 15 \pmod{16}$ and $(-1)^{\frac{l+1}{16}}(\frac{2u}{v}) = -1$, where $(u, v) \in \mathbb{Z}_{>0}^2$ satisfying $l = u^2 - 2v^2$.*

We have the following theorem.

Theorem 3.7. *Assume that $l \equiv 7 \pmod 8$ is a prime. Then $\mathcal{T}_2(l)$ and $\mathcal{T}_2(2l)$ are nontrivial 2-cyclic groups, $4 \mid t_2(l)$ and*

(1) *$t_2(l) = 4 \Leftrightarrow t_2(2l) = 2 \Leftrightarrow h_2(-2l) = 4 \Leftrightarrow l \equiv 7 \pmod{16}$;*

(2) *$t_2(l) = 8 \Leftrightarrow t_2(2l) = 4 \Leftrightarrow h_2(-2l) = 8 \Leftrightarrow l \equiv 15 \pmod{16}$ and $(-1)^{\frac{l+1}{16}}(\frac{2u}{v}) = -1$, where $(u, v) \in \mathbb{Z}_{>0}^2$ is a solution of $l = X^2 - 2Y^2$.*

Consequently, we always have $t_2(l) \equiv 2t_2(2l) \equiv h_2(-2l) \pmod{16}$.

Remark 3.8. However, in general the three numbers $t_2(l)$, $2t_2(2l)$ and $h_2(-2l)$ are not equal if one (hence all) of them is greater than or equal to 16. For example, let $l = 223$. Then $t_2(l) = 16$, $2t_2(2l) = 256$ and $h_2(-2l) = 32$.

Proof of Theorem 3.7. (1) We first study $t_2(l)$. As shown in the proof of Lemma 3.4,

$$\varepsilon_l = a_l + b_l\sqrt{l} = \frac{1}{2}(c + d\sqrt{l})^2,$$

where c and d are odd integers and $N(c + d\sqrt{l}) = c^2 - d^2 l = 2$. In particular, $c^2 \equiv 2 \pmod d$. It follows that every prime factor of d is congruent to $\pm 1 \pmod 8$. Hence $d^2 \equiv 1 \pmod{16}$ and $\nu_2(a_l) = \nu_2(1+d^2 l)$. For $l \equiv 7 \pmod 8$, $\nu_2(1 + d^2 l) \geqslant 3$ with the equality if and only if $l \equiv 7 \pmod{16}$. By Lemma 3.4(1), $4 \mid t_2(l) = 2^{\nu_2(ld^2+1)-1}$, and $t_2(l) = 4$ if and only if $l \equiv 7 \pmod{16}$.

Note that the Jacobi symbol $(\frac{2u}{v})$ is independent of the choices of u and v (see [15, Lemma 4.1]). By the results of Leonard and Williams [13] (Proposition 3.6(2)), we are left to show that if $l \equiv 15 \pmod{16}$, then

$$\nu_2(ld^2 + 1) = 4 \Leftrightarrow (-1)^{\frac{l+1}{16}}\left(\frac{2u}{v}\right) = -1.$$

Since $l = (u+\sqrt{2}v)(u-\sqrt{2}v) \mid ld^2 = (c+\sqrt{2})(c-\sqrt{2})$, one of the prime elements $u \pm \sqrt{2}v$ must divides $c + \sqrt{2}$ in the Euclidean domain $\mathbb{Z}[\sqrt{2}]$.

(i) Suppose $\frac{c+\sqrt{2}}{u+\sqrt{2}v} \in \mathbb{Z}[\sqrt{2}]$. Note that $c+\sqrt{2}$ and $c-\sqrt{2}$ are coprime in $\mathbb{Z}[\sqrt{2}]$, and the integers $\frac{c+\sqrt{2}}{u+\sqrt{2}v}$ and $\frac{c-\sqrt{2}}{u-\sqrt{2}v}$ are coprime, but their product is d^2 and $\mathbb{Z}[\sqrt{2}]$ has class number 1, and hence there exist $s,t\in\mathbb{Z}$ and $\varepsilon\in\{1,1+\sqrt{2}\}$ such that

$$\frac{c+\sqrt{2}}{u+\sqrt{2}v}=\varepsilon(t-s\sqrt{2})^2.$$

Since the left-hand side is totally positive, we must have $\varepsilon=1$. Comparing the coefficients of $\sqrt{2}$ gives

$$1=(t^2+2s^2)v-2tsu. \tag{3.2}$$

Note that ts must be positive. We may assume that t and s are both positive. Since $l=u^2-2v^2\equiv-1 \pmod{16}$, both u and v are odd. In fact, $v\equiv1 \pmod 4$ by (3.2). Hence $(\frac{2u}{v})=(\frac{-st}{v})=(\frac{t}{v})(\frac{s}{v})$. Note that d and t are odd. By the quadratic reciprocity law, $(\frac{t}{v})=(\frac{v}{t})=(\frac{2}{t})$. The last equality follows from (3.2). Write $s=2^r s_0$ with $2\nmid s_0$. If $s\equiv 2 \pmod 4$, then $v\equiv 5 \pmod 8$ and $(\frac{s}{v})=(\frac{2\cdot s_0}{v})=-(\frac{v}{s_0})$. If $s\equiv 0 \pmod 4$, then $t^2\equiv 1 \pmod 8$ and $v\equiv 1 \pmod 8$. So $(\frac{s}{v})=(\frac{s_0}{v})=(\frac{v}{s_0})=1$. If $s\equiv\pm1 \pmod 4$, then $(\frac{s}{v})=(\frac{v}{s})=1$. Hence,

$$\left(\frac{s}{v}\right)=\begin{cases}-1, & \text{if } s\equiv 2 \pmod 4,\\ 1, & \text{otherwise.}\end{cases}$$

Therefore, $(\frac{2u}{v})=1$ if and only if $\pm d=t^2-2s^2\equiv\pm1 \pmod{16}$. This implies that $16\parallel ld^2+1$ if and only if $(-1)^{\frac{l+1}{16}}(\frac{2u}{v})=-1$.

(ii) Suppose $\frac{c+\sqrt{2}}{u-\sqrt{2}v}\in\mathbb{Z}[\sqrt{2}]$. By the similar argument, there exist two positive integers t and s such that

$$1=2stu-(t^2+2s^2)v.$$

For this equation, $v\equiv 3 \pmod 4$ and $(\frac{2u}{v})=(\frac{t}{v})(\frac{s}{v})$. One can repeat the argument above to obtain that $(\frac{t}{v})=(\frac{2}{t})$ and

$$\left(\frac{s}{v}\right)=\begin{cases}-1, & \text{if } s\equiv 2 \pmod 4,\\ 1, & \text{otherwise.}\end{cases}$$

Again this implies that $16\parallel ld^2+1$ if and only if $(-1)^{\frac{l+1}{16}}(\frac{2u}{v})=-1$.

(2) If $l\equiv 7 \pmod 8$, then $h(2l)$ is odd. By Lemma 3.4(2), $\nu_2(t_2(2l))=\nu_2(b_{2l})-1$. According to the last paragraph in [13, Section 3], we have $h(-2l)\equiv b_{2l} \pmod{16}$. Then

$$t_2(2l)=\frac{h_2(-2l)}{2}=\frac{t_2(l)}{2},$$

if t_{2l} equals 2 or 4. We just need to apply Proposition 3.6. □

Proposition 3.9. *Assume that $l\equiv 1 \pmod 8$ is a prime.*

(1) *Write $l=2g^2-h^2$ with $g,h\in\mathbb{Z}_{>0}$. Then*

$$t_2(l)=2\Leftrightarrow h_2(-l)=4\Leftrightarrow g\equiv 3 \pmod 4, \tag{3.3}$$

$$t_2(l)=4\Leftrightarrow\begin{cases}h_2(-l)=8, & \text{if } l\equiv 1 \pmod{16},\\ h_2(-l)\geqslant 16, & \text{if } l\equiv 9 \pmod{16}\end{cases}\Leftrightarrow(-1)^{\frac{l-1}{8}}\left(\frac{2h}{g}\right)\left(\frac{g}{l}\right)_4=-1. \tag{3.4}$$

(2) *Write $l=u^2-2v^2$ with $u,v\in\mathbb{Z}_{>0}$ and $u\equiv 1 \pmod 4$. Then*

$$t_2(2l)=2\Leftrightarrow\left(\frac{u}{l}\right)=-1, \tag{3.5}$$

$$t_2(2l)=4\Leftrightarrow(-1)^{\frac{l-1}{8}}\left(\frac{u}{l}\right)_4=-1. \tag{3.6}$$

Proof. (1) For $l \equiv 1 \pmod 8$, Williams [23] proved that

$$a_l \equiv \begin{cases} h(-l)+l-1 \pmod{16}, & \text{if } h_2(-l) \geqslant 8, \\ 4(h(l)-1)+l-1-h(-l) \pmod{16}, & \text{if } h_2(-l)=4. \end{cases}$$

Hence we have

$$\begin{cases} 2t_2(l) \equiv h(-l)+l-1 \pmod{16}, & \text{if } h_2(-l) \geqslant 8, \\ t_2(l)=2, & \text{if } h_2(-l)=4. \end{cases} \tag{3.7}$$

Applying Coates' order formula (3.1), Lemma 3.4 and Proposition 3.6(1), we get the result.

(2) It follows from (3.1) that $t_2(2l)$ is equal to $\log_2(\varepsilon_{2l})h(2l)/(2\sqrt{2})$ up to a 2-adic unit. Denote by $R+S\sqrt{2l}$ the fundamental unit of norm 1 of $\mathbb{Q}(\sqrt{2l})$ and by $h^+(2l)$ the narrow class number of $\mathbb{Q}(\sqrt{2l})$. Then $R+S\sqrt{2l}=\varepsilon_{2l}$ and $h^+(2l)=2h(2l)$ if $N(\varepsilon_{2l})=1$; $R+S\sqrt{2l}=\varepsilon_{2l}^2$ and $h^+(2l)=h(2l)$ if $N(\varepsilon_{2l})=-1$. Thus, by Lemma 3.4(2), we have

$$\nu_2(t_2(2l)) = \nu_2(h^+(2l)) + \nu_2(S) - 2.$$

The main theorem in [10] tells us that

$$\frac{S\cdot h^+(2l)}{2} \equiv 1-l-h(-2l) \pmod{16}.$$

Then all the results here directly follow the discussion in [13, Section 2]. $\square$

Now we can prove the density results about $\mathcal{T}_2(l)$ and $\mathcal{T}_2(2l)$.

Proof of Theorem 1.3. (1) We first show (1.4). In the case $e=0$, then $l \equiv 1 \pmod 8$. Stevenhagen [21, Theorem 1] proved that $h_2(-l) \geqslant 8$ if and only if l splits completely in $\mathbb{Q}(\zeta_8, \sqrt{1+i})$. Then by Chebotarev's density theorem,

$$\lim_{x\to\infty} \frac{\#\{l \leqslant x : l \equiv 1 \pmod 8, h_2(-l)=4\}}{\#\{l \leqslant x : l \equiv 1 \pmod 8\}} = \lim_{x\to\infty} \frac{\#\{l \leqslant x : l \equiv 1 \pmod 8, h_2(-l)\geqslant 8\}}{\#\{l \leqslant x : l \equiv 1 \pmod 8\}} = \frac{1}{2}.$$

By (3.3) in Proposition 3.9, the case $i=0$ follows.

Recently, Koymans [11, Theorem 1.1] proved that

$$\lim_{x\to\infty} \frac{\#\{l \leqslant x : l \equiv 1 \pmod 8, h_2(-l)=8\}}{\#\{l \leqslant x : l \equiv 1 \pmod 8\}} = \frac{1}{4}.$$

As a corollary of [21, Theorem 1], we have that $l \equiv 9 \pmod{16}$ such that $h_2(-l) \geqslant 8$ if and only if the Frobenius of l in $\mathrm{Gal}(\mathbb{Q}(\zeta_{16}, \sqrt{1+i})/\mathbb{Q})$ acts trivially in $\mathbb{Q}(\zeta_8, \sqrt{1+i})$ and maps ζ_{16} to $-\zeta_{16}$. Hence,

$$\lim_{x\to\infty} \frac{\#\{l \leqslant x : l \equiv 9 \pmod{16}, h_2(-l)\geqslant 8\}}{\#\{l \leqslant x : l \equiv 9 \pmod{16}\}} = \lim_{x\to\infty} \frac{\#\{l \leqslant x : l \equiv 1 \pmod{16}, h_2(-l)\geqslant 8\}}{\#\{l \leqslant x : l \equiv 1 \pmod{16}\}} = \frac{1}{2}.$$

If we can show

$$\lim_{x\to\infty} \frac{\#\{l \leqslant x : l \equiv 9 \pmod{16}, h_2(-l)=8\}}{\#\{l \leqslant x : l \equiv 9 \pmod{16}\}} = \lim_{x\to\infty} \frac{\#\{l \leqslant x : l \equiv 9 \pmod{16}, h_2(-l)\geqslant 16\}}{\#\{l \leqslant x : l \equiv 9 \pmod{16}\}} = \frac{1}{4}, \tag{3.8}$$

then

$$\lim_{x\to\infty} \frac{\#\{l \leqslant x : l \equiv 1 \pmod{16}, h_2(-l)\geqslant 16\}}{\#\{l \leqslant x : l \equiv 1 \pmod{16}\}} = \lim_{x\to\infty} \frac{\#\{l \leqslant x : l \equiv 1 \pmod{16}, h_2(-l)=8\}}{\#\{l \leqslant x : l \equiv 1 \pmod{16}\}} = \frac{1}{4}.$$

Hence the case $i=1$ follows from (3.4). It suffices to show (3.8).

Let

$$e_l = \begin{cases} 1, & \text{if } h_2(-l) \geqslant 16, \\ -1, & \text{if } h_2(-l) = 8, \\ 0, & \text{if } h_2(-l) = 4. \end{cases}$$

By [11, Theorem 1.2], we have

$$\sum_{l \leqslant x, l \equiv 1 \pmod 8} e_l \ll x/\exp((\log x)^{0.1}). \tag{3.9}$$

Replacing the spin symbol $[w]$ in [11, Lemmas 4.1 and 4.2] by the twisted symbol $[w]' := [w] \cdot \lambda(w)$ for all the totally positive elements w of $\mathbb{Z}[\zeta_8]$, where $\lambda(w)$ equals $(-1)^{\frac{Nw-1}{8}}$ if $Nw \equiv 1 \pmod 8$ and 1 otherwise, one follows the argument there and obtains

$$\sum_{l \leqslant x, l \equiv 1 \pmod 8} (-1)^{\frac{l-1}{8}} e_l \ll x/\exp((\log x)^{0.1}). \tag{3.10}$$

Thus

$$\sum_{l \leqslant x, l \equiv 1 \pmod 8} (e_l - (-1)^{\frac{l-1}{8}} e_l) = 2 \sum_{l \leqslant x, l \equiv 9 \pmod{16}} (1_{16 \mid h(-l)} - 1_{8 \,\|\, h(-l)}) \ll x/\exp((\log x)^{0.1}).$$

Note that as $x \to +\infty$, $\log x = o(\exp((\log x)^{0.1}))$. By Dirichlet's density theorem, we have

$$\#\{l \leqslant x,\, l \equiv 9 \pmod{16},\, h_2(-l) = 8\} \sim \#\{l \leqslant x,\, l \equiv 9 \pmod{16},\, h_2(-l) \geqslant 16\} \sim \frac{x}{32 \log x}.$$

Hence we have (3.8).

In the case $e = 1$, $l \equiv 7 \pmod 8$. By Theorem 3.7, the case $i = 0$ follows from the fact that $t_2(l) = 4$ if and only if $l \equiv 7 \pmod{16}$, and the case $i = 1$ follows from the following result of Milovic [17, Theorem 1] on $h_2(-2l)$ that

$$\lim_{x \to \infty} \frac{\#\{l \leqslant x : l \equiv -1 \pmod 8, h_2(-2l) = 8\}}{\#\{l \leqslant x : l \equiv -1 \pmod 8\}} = \frac{1}{4}.$$

(2) Case 7 (mod 8) for (1.5) follows from (1) and Theorem 3.7, and Case 1 (mod 8) follows from Proposition 3.9(2) and [12, Theorem 1] with the similar arguments for $t_2(l)$; we omit the details. □

Remark 3.10. We actually proved that for the cases where $i = 1$ and $i = 2$,

$$\lim_{x \to \infty} \frac{\#\{l \leqslant x : l \equiv 1 \pmod{16}, t_2(l) = 2^i\}}{\#\{l \leqslant x : l \equiv 1 \pmod{16}\}} = \lim_{x \to \infty} \frac{\#\{l \leqslant x : l \equiv 9 \pmod{16}, t_2(l) = 2^i\}}{\#\{l \leqslant x : l \equiv 9 \pmod{16}\}} = \frac{1}{2^i}.$$

4 Distribution conjectures for $\mathcal{T}_p$-groups of quadratic fields

4.1 Distribution conjecture of $\mathcal{T}_p$ in the full family

We first propose a distribution conjecture on the group structure of $\mathcal{T}_p(F)$ when F varies in the family of all the imaginary (resp. real) quadratic fields $\mathcal{F}_{\mathrm{im}}$ (resp. $\mathcal{F}_{\mathrm{re}}$).

For $5 \leqslant p \leqslant 47$, the numerical data presented in [18, Subsection 5.2] suggested that of all the real quadratic fields $\mathbb{Q}(\sqrt{m})$ with $m \leqslant 10^9$ squarefree, the proportion of those with trivial $\mathcal{T}_p$-groups (namely the so-called p-rational fields) is close to $\eta_\infty(p)$. It was mentioned there that the authors also considered the distribution about the group structures of $\mathcal{T}_p$-groups, however, we did not find any further statement and subsequent studies in the literature.

Based on Theorem 1.1 and the numerical data in the appendixes, we propose the following conjecture.

Conjecture 4.1. Let p be a prime. Let $\mathcal{F}_{\mathrm{im}}$ (resp. $\mathcal{F}_{\mathrm{re}}$) be the family of all the imaginary (resp. real) quadratic fields. For each finite abelian p-group G, one has

$$\lim_{x \to \infty} \frac{\#\{F \in \mathcal{F}_{\mathrm{im}} \mid -D_F \leqslant x, 6\mathcal{T}_p(F) \cong G\}}{\#\{F \in \mathcal{F}_{\mathrm{im}} : -D_F \leqslant x\}} = \frac{\eta_\infty(p)/\eta_1(p)}{\#G \cdot \#\mathrm{Aut}(G)}, \tag{4.1}$$

$$\lim_{x\to\infty}\frac{\#\{F\in\mathcal{F}_{\rm re}\mid D_F\leqslant x, 6\mathcal{T}_p(F)\cong G\}}{\#\{F\in\mathcal{F}_{\rm re}: D_F\leqslant x\}}=\frac{\eta_\infty(p)}{\#\mathrm{Aut}(G)}. \tag{4.2}$$

Here, D_F is the discriminant of F, and we recall that $\eta_s(q):=\prod_{i=1}^{s}(1-q^{-i})$ for $s\in\mathbb{Z}_{>0}\cup\{\infty\}$ and $q>1$.

Remark 4.2. (1) For $p\geqslant 5$, we have $6\mathcal{T}_p(F)\cong\mathcal{T}_p(F)$, and hence the factor 6 can be removed from the statement of our conjecture. For p equal to 2 and 3, we have $6\mathcal{T}_p(F)=p\mathcal{T}_p(F)$. For p equal to 5 and 7, we have carried out numerical computations of $\mathcal{T}_p(F)$ with $|D_F|\leqslant 5\times 10^7$ (see Tables 1–4 in Appendix A), which give strong evidence of Conjecture 4.1 in these cases.

(2) For the bad primes 2 and 3, when the bound is 5×10^7, the distributions of $2\mathcal{T}_2$ and $3\mathcal{T}_3$ are actually not quite good based on our computation, but this is expected just like the analogue phenomenon for the distributions of narrow 2-class groups and tame kernels of quadratic fields: the bound is not big enough. We gain confidence from recent breakthrough of Smith [20] on the distribution of narrow 2-class groups of quadratic fields, as well as the 4-rank density formula for $\mathcal{T}_2$ of imaginary quadratic fields we just proved here.

(3) If we use the setting of the local Cohen-Lenstra heuristics, we have that the weight function for p-class groups is ω_0 for imaginary quadratic fields and ω_1 for real ones where

$$\omega_i(G)=\frac{1}{(\#G)^i\cdot\#\mathrm{Aut}(G)}, \tag{4.3}$$

and the weight functions for $\mathcal{T}_p$-groups are exactly the reverse order.

(4) For more general conjectures on distributions of $\mathcal{T}_p$-groups of quadratic fields, which are also in the spirit of the Cohen-Lenstra heuristics, please see [14].

4.2 Distribution conjecture of $\mathcal{T}_2$ in sub-families

Conjecture 4.3. Assume that all l's appeared below are primes. For each integer $i\geqslant 0$ and $e\in\{0,1\}$, we have

$$\lim_{x\to\infty}\frac{\#\{l\leqslant x: l\equiv 1 \pmod{16}, t_2(-l)=2^{i+3}\}}{\#\{l\leqslant x: l\equiv 1 \pmod{16}\}}=\frac{3}{4^{i+1}}, \tag{4.4}$$

$$\lim_{x\to\infty}\frac{\#\{l\leqslant x: l\equiv 1 \pmod{16}, t_2(-2l)=2^{i+2}\}}{\#\{l\leqslant x: l\equiv 1 \pmod{16}\}}=\frac{3}{4^{i+1}}, \tag{4.5}$$

$$\lim_{x\to\infty}\frac{\#\{l\leqslant x: l\equiv (-1)^e \pmod{8}, t_2(l)=2^{i+1+e}\}}{\#\{l\leqslant x: l\equiv (-1)^e \pmod{8}\}}=\frac{1}{2^{i+1}}, \tag{4.6}$$

$$\lim_{x\to\infty}\frac{\#\{l\leqslant x: l\equiv (-1)^e \pmod{8}, t_2(2l)=2^{i+1}\}}{\#\{l\leqslant x: l\equiv (-1)^e \pmod{8}\}}=\frac{1}{2^{i+1}}. \tag{4.7}$$

We shall present the numerical evidence in Tables 5–10 in Appendix B.

Remark 4.4. (1) Under the setting of the extended local Cohen-Lenstra heuristics, one can interpret (4.4) more conceptually as follows. Let

$$\mathcal{M}_k=\{\mathbb{Z}/2^{i+k}\mathbb{Z}\mid i\geqslant 0\}\quad\text{for } k\geqslant 1.$$

For $G=\mathbb{Z}/2^{i+k}\mathbb{Z}\in\mathcal{M}_k$, then a direct computation gives

$$\frac{\omega_1(G)}{\sum_{H\in\mathcal{M}_k}\omega_1(H)}=\frac{3}{4^{i+1}}.$$

Thus, (4.4) is equivalent to that the natural density of primes l with $\mathcal{T}_2(-l)\cong G$ among all the primes $\equiv 1 \pmod{16}$ is equal to the ratio of $\omega_1(G)$ to the total 1-weight of the space $\mathcal{M}_3$. For (4.5), the corresponding space is $\mathcal{M}_2$.

(2) One can also reformulate (4.6) and (4.7) by using the weight function ω_0 and by noting the following identity:

$$\frac{\omega_0(G)}{\sum_{H\in\mathcal{M}_k}\omega_0(H)}=\frac{1}{2^{i+1}},\quad \text{where } G=\mathbb{Z}/2^{k+i}\mathbb{Z}.$$

In (4.6) (resp. (4.7)), the total space is $\mathcal{M}_{e+1}$ (resp. $\mathcal{M}_1$).

(3) By Lemma 3.4(1), (4.6) has the following equivalent form about the distribution of fundamental units: for each $i\geqslant 0$ and $e\in\{0,1\}$,

$$\lim_{x\to\infty}\frac{\#\{l \text{ prime}: l\leqslant x, l\equiv(-1)^e \pmod 8, \nu_2(a_l)=i+2+e\}}{\#\{l \text{ prime}: l\leqslant x, l\equiv(-1)^e \pmod 8\}}=\frac{1}{2^{i+1}}. \tag{4.8}$$

(4) Finally, for $l\equiv 1 \pmod 8$, (4.6) actually has a finer form: for $i\geqslant 0$ and $a\in\{1,9\}$,

$$\lim_{x\to\infty}\frac{\#\{l\leqslant x: l\equiv a \pmod{16}, t_2(l)=2^{i+1}\}}{\#\{l\leqslant x: l\equiv a \pmod{16}\}}=\frac{1}{2^{i+1}}. \tag{4.9}$$

The cases where $i=0$ and $i=1$ were proved in Theorem 1.3. We actually speculate that this is the case for all the sub-congruent classes $a \pmod{2^k}$ of $1 \pmod 8$.

In the case $a=9$, let χ_l be the associated Dirichlet character of $\mathbb{Q}(\sqrt{l})$ and $L_2(s,\chi_l)$ be its 2-adic L-function. By the 2-adic class number formula (see [22, Theorem 5.24]) and Coates' order formula (3.1), (4.9) has the following equivalent form which was implicitly proposed by Shanks et al. [19, p. 1253]:

$$\lim_{x\to\infty}\frac{\#\{l \text{ prime}: l\leqslant x, l\equiv 9 \pmod{16} \text{ and } \nu_2(L_2(1,\chi_l))=i+2\}}{\#\{l \text{ prime}: l\leqslant x \text{ and } l\equiv 9 \pmod{16}\}}=\frac{1}{2^{i+1}}. \tag{4.10}$$

Acknowledgements This work was supported by Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200). The authors are grateful to the referees for their very helpful suggestions and remarks.

References

1 Brown E A. The class number of $\mathbb{Q}(\sqrt{-p})$, for $p\equiv 1 \pmod 8$ a prime. Proc Amer Math Soc, 1972, 31: 381–383
2 Coates J H. p-adic L-functions and Iwasawa's theory. In: Algebraic Number Fields: L-Functions and Galois Properties. London: Academic Press, 1977, 269–353
3 Colmez P. Résidu en $s=1$ des fonctions zêta p-adiques. Invent Math, 1988, 91: 371–389
4 Cox D A. Primes of the Form x^2+ny^2, 2nd ed. Fermat, Class Field Theory, and Complex Multiplication. Hoboken: John Wiley & Sons, 2013
5 Gerth III F. The 4-class ranks of quadratic fields. Invent Math, 1984, 77: 489–515
6 Gras G. Groupe de Galois de la p-extension abélienne p-ramifiée maximale d'un corps de nombres. J Reine Angew Math, 1982, 333: 86–132
7 Gras G. Class Field Theory: From Theory to Practice. Springer Monographs in Mathematics. Berlin: Springer-Verlag, 2003
8 Gras G. Practice of the incomplete p-ramification over a number field—History of abelian p-ramification. Comm Adv Math Sci, 2019, 2: 251–280
9 Hasse H. Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p\neq 2$. J Number Theory, 1969, 1: 231–234
10 Kaplan P, Williams K S. On the class numbers of $\mathbb{Q}(\sqrt{\pm 2p})$ modulo 16, for $p\equiv 1 \pmod 8$ a prime. Acta Arith, 1982, 40: 289–296
11 Koymans P. The 16-rank of $\mathbb{Q}(\sqrt{-p})$. Algebra Number Theory, 2020, 14: 37–65
12 Koymans P, Milovic D. On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-2p})$ for primes $p\equiv 1 \pmod 4$. Int Math Res Not IMRN, 2019, 23: 7406–7427
13 Leonard P A, Williams K S. On the divisibility of the class numbers of $\mathbb{Q}(\sqrt{-p})$ and $\mathbb{Q}(\sqrt{-2p})$ by 16. Canad Math Bull, 1982, 25: 200–206
14 Li J N, Ouyang Y, Xu Y. Abelian p-ramification groups and new Cohen-Lenstra heuristics (in Chinese). Sci Sin Math, 2021, 51: 1635–1654
15 Li J N, Xu Y. On class numbers of pure quartic fields. Ramanujan J, 2021, 56: 235–248
16 Li J N, Yu C F. The Chevalley-Gras formula over global fields. J Theor Nombres Bordeaux, 2020, 32: 525–543
17 Milovic D. On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-8p})$ for $p\equiv -1 \pmod 4$. Geom Funct Anal, 2017, 27: 973–1016

18 Pitoun F, Varescon F. Computing the torsion of the p-ramified module of a number field. Math Comp, 2015, 84: 371–383
19 Shanks D C, Sime P J, Washington L C. Zeros of 2-adic L-functions and congruences for class numbers and fundamental units. Math Comp, 1999, 68: 1243–1255
20 Smith A. 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. arXiv:1702.02325v2, 2017
21 Stevenhagen P. Divisibility by 2-powers of certain quadratic class numbers. J Number Theory, 1993, 43: 1–19
22 Washington L C. Introduction to Cyclotomic Fields. Graduate Texts in Mathematics, vol. 83. New York: Springer, 1997
23 Williams K S. On the class number of $\mathbb{Q}(\sqrt{-p})$ modulo 16, for $p \equiv 1 \pmod 8$ a prime. Acta Arith, 1981, 39: 381–398
24 Yue Q, Yu J. The densities of 4-ranks of tame kernels for quadratic fields. J Reine Angew Math, 2004, 567: 151–173
25 Zhang Z, Yue Q. Fundamental units of real quadratic fields of odd class number. J Number Theory, 2014, 137: 122–129

Appendix A Data for Conjecture 4.1

In Tables 1–4, we let the middle value be the ratio of the field F such that $\mathcal{T}_p(F) \cong G$ among all the quadratic fields whose absolute discriminant is less than or equal to B, and $\mathbb{D}$ be the value predicted by Conjecture 4.1.

Table 1 $\mathcal{T}_5$ of real quadratic fields

B \ G	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/25\mathbb{Z}$	$(\mathbb{Z}/5\mathbb{Z})^2$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$	$(\mathbb{Z}/5\mathbb{Z})^3$
10^7	0.1876	0.03694	1.375E−3	3.277E−4	0
2×10^7	0.1880	0.03712	1.396E−3	3.463E−4	1.645E−7
3×10^7	0.1880	0.03727	1.416E−3	3.439E−4	2.193E−7
4×10^7	0.1880	0.03739	1.438E−3	3.447E−4	3.290E−7
5×10^7	0.1882	0.03740	1.453E−3	3.430E−4	2.632E−7
$\mathbb{D}$	0.1901	0.03802	1.584E−3	3.802E−4	5.110E−7

Table 2 $\mathcal{T}_7$ of real quadratic fields

B \ G	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Z}/49\mathbb{Z}$	$(\mathbb{Z}/7\mathbb{Z})^2$	$(\mathbb{Z}/7\mathbb{Z})^3$
10^7	0.1377	0.01950	3.622E−4	0
2×10^7	0.1382	0.01956	3.622E−4	0
3×10^7	0.1383	0.01963	3.713E−4	0
4×10^7	0.1385	0.01966	3.764E−4	0
5×10^7	0.1385	0.01968	3.833E−4	5.483E−8
$\mathbb{D}$	0.1395	0.01992	4.151E−4	2.477E−8

Table 3 $\mathcal{T}_5$ of imaginary quadratic fields

B \ G	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/25\mathbb{Z}$	$(\mathbb{Z}/5\mathbb{Z})^2$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$	$(\mathbb{Z}/5\mathbb{Z})^3$
10^7	0.04558	1.767E−3	6.185E−5	6.580E−7	0
2×10^7	0.04584	1.789E−3	6.004E−5	1.645E−6	0
3×10^7	0.04604	1.801E−3	6.152E−5	2.084E−6	0
4×10^7	0.04613	1.809E−3	6.424E−5	2.385E−6	0
5×10^7	0.04618	1.915E−3	6.659E−5	2.237E−6	0
$\mathbb{D}$	0.04752	1.901E−3	7.920E−5	3.802E−6	5.110E−9

Table 4 $\mathcal{T}_7$ of imaginary quadratic fields

B \ G	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Z}/49\mathbb{Z}$	$(\mathbb{Z}/7\mathbb{Z})^2$	$(\mathbb{Z}/7\mathbb{Z})^3$
10^7	0.02287	0.00043	3.619E−6	0
2×10^7	0.02297	0.00045	5.263E−6	0
3×10^7	0.02302	0.00045	5.593E−6	0
4×10^7	0.02307	0.00045	6.827E−6	0
5×10^7	0.02307	0.00045	7.435E−6	0
$\mathbb{D}$	0.02324	0.00047	9.883E−6	8.425E−11

Appendix B Data for Conjecture 4.3

In Tables 5–10, we let the middle value be the ratio of the field F such that $\mathcal{T}_p(F)\cong G$ among all the quadratic fields whose absolute discriminant is less than or equal to B, and $\mathbb{D}$ be the value predicted by Conjecture 4.3.

Table 5 $\mathcal{T}_2$ of $\mathbb{Q}(\sqrt{-l})$, $l\equiv 1 \pmod{16}$ and l is a prime

B \ G	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/16\mathbb{Z}$	$\mathbb{Z}/32\mathbb{Z}$	$\mathbb{Z}/64\mathbb{Z}$	$\mathbb{Z}/128\mathbb{Z}$
10^7	0.7508	0.1867	0.04704	0.01172	2.905E−3
2×10^7	0.7501	0.1872	0.04708	0.01170	3.062E−3
3×10^7	0.7501	0.1878	0.04658	0.01169	2.977E−3
4×10^7	0.7498	0.1881	0.04666	0.01166	2.910E−3
5×10^7	0.7496	0.1880	0.04694	0.01160	2.934E−3
$\mathbb{D}$	0.7500	0.1875	0.04688	0.01172	2.930E−3

Table 6 $\mathcal{T}_2$ of $\mathbb{Q}(\sqrt{-2l})$, $l\equiv 1 \pmod{16}$ and l is a prime

B \ G	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/16\mathbb{Z}$	$\mathbb{Z}/32\mathbb{Z}$	$\mathbb{Z}/64\mathbb{Z}$
10^7	0.7508	0.1876	0.04611	0.01144	3.134E−3
2×10^7	0.7501	0.1886	0.04604	0.01142	3.075E−3
3×10^7	0.7501	0.1885	0.04611	0.01140	3.029E−3
4×10^7	0.7498	0.1885	0.04633	0.01153	3.032E−3
5×10^7	0.7496	0.1883	0.04655	0.01157	3.051E−3
$\mathbb{D}$	0.7500	0.1875	0.04688	0.01172	2.930E−3

Table 7 $\mathcal{T}_2$ of $\mathbb{Q}(\sqrt{l})$, $l\equiv 1 \pmod{8}$ and l is a prime

B \ G	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/16\mathbb{Z}$	$\mathbb{Z}/32\mathbb{Z}$	$\mathbb{Z}/64\mathbb{Z}$
10^7	0.5002	0.2499	0.1245	0.06236	0.03169	0.01553
2×10^7	0.5000	0.2499	0.1245	0.06255	0.03163	0.01567
3×10^7	0.5005	0.2496	0.1246	0.06278	0.03115	0.01560
4×10^7	0.5003	0.2496	0.1247	0.06278	0.03115	0.01564
5×10^7	0.5001	0.2497	0.1247	0.06281	0.03116	0.01567
$\mathbb{D}$	0.5000	0.2500	0.1250	0.06250	0.03125	0.01563

Table 8 $\mathcal{T}_2$ of $\mathbb{Q}(\sqrt{l})$, $l \equiv 7 \pmod 8$ and l is a prime

B \ G	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/16\mathbb{Z}$	$\mathbb{Z}/32\mathbb{Z}$	$\mathbb{Z}/64\mathbb{Z}$	$\mathbb{Z}/128\mathbb{Z}$
10^7	0.5000	0.2484	0.1260	0.06361	0.03103	0.01518
2×10^7	0.5000	0.2494	0.1255	0.06265	0.03123	0.01534
3×10^7	0.4998	0.2497	0.1252	0.06278	0.03109	0.01557
4×10^7	0.4999	0.2497	0.1254	0.06246	0.03112	0.01570
5×10^7	0.5001	0.2497	0.1254	0.06237	0.03116	0.01570
$\mathbb{D}$	0.5000	0.2500	0.1250	0.06250	0.03125	0.01563

Table 9 $\mathcal{T}_2$ of $\mathbb{Q}(\sqrt{2l})$, $l \equiv 1 \pmod 8$ and l is a prime

B \ G	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/16\mathbb{Z}$	$\mathbb{Z}/32\mathbb{Z}$	$\mathbb{Z}/64\mathbb{Z}$
10^7	0.5006	0.2515	0.1237	0.06214	0.03100	0.01564
2×10^7	0.5004	0.2511	0.1239	0.06219	0.03105	0.01576
3×10^7	0.5001	0.2506	0.1245	0.06256	0.03093	0.01572
4×10^7	0.5001	0.2505	0.1249	0.06233	0.03090	0.01564
5×10^7	0.5000	0.2503	0.1252	0.06236	0.03083	0.01572
$\mathbb{D}$	0.5000	0.2500	0.1250	0.06250	0.03125	0.01563

Table 10 $\mathcal{T}_2$ of $\mathbb{Q}(\sqrt{2l})$, $l \equiv 7 \pmod 8$ and l is a prime

B \ G	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/16\mathbb{Z}$	$\mathbb{Z}/32\mathbb{Z}$	$\mathbb{Z}/64\mathbb{Z}$
10^7	0.5000	0.2484	0.1253	0.06378	0.03129	0.01565
2×10^7	0.5000	0.2.494	0.1253	0.06258	0.03137	0.01565
3×10^7	0.4998	0.2497	0.1254	0.06258	0.03116	0.01575
4×10^7	0.4999	0.2497	0.1252	0.06267	0.03129	0.01569
5×10^7	0.5001	0.2497	0.1250	0.06268	0.03126	0.01573
$\mathbb{D}$	0.5000	0.2500	0.1250	0.06250	0.03125	0.01563