*J. Inst. Math. Jussieu* (2022), **21**(5), 1543–1570
doi:10.1017/S1474748020000651 
Published by Cambridge University Press.



# ON THE 4-RANK OF CLASS GROUPS OF DIRICHLET BIQUADRATIC FIELDS

ÉTIENNE FOUVRY [1], PETER KOYMANS [2] AND CARLO PAGANO [3]

[1] *Université Paris–Saclay, CNRS, Laboratoire de mathématiques d'Orsay, 91405 Orsay, France* (Etienne.Fouvry@universite-paris-saclay.fr)
[2] *Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany* (koymans@mpim-bonn.mpg.de)
[3] *Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany* (carlein90@gmail.com)

(Received 24 June 2020; revised 7 October 2020; accepted 9 October 2020; first published online 22 December 2020)

*Abstract* We show that for 100% of the odd, square free integers $n > 0$, the 4-rank of $\mathrm{Cl}(\mathbb{Q}(i, \sqrt{n}))$ is equal to $\omega_3(n) - 1$, where $\omega_3$ is the number of prime divisors of $n$ that are 3 modulo 4.

*Keywords and phrases*: class groups; arithmetic statistics; biquadratic fields

2020 *Mathematics Subject Classification*: Primary 11N45
Secondary 11R29

## 1. Introduction

A classical result in number theory is the theorem of Gauss on ambiguous binary quadratic forms. This theorem gives, in modern terms, a description of $\mathrm{Cl}(K)[2]$ if $K$ is a quadratic extension of $\mathbb{Q}$. In particular, Gauss proved that the dimension of the $\mathbb{F}_2$-vector space $\mathrm{Cl}(K)[2]$ equals $\omega(\Delta_K) - 1$, where $\omega(\cdot)$ is the number of distinct prime divisors, $\mathrm{Cl}(K)$ is the narrow class group and $\Delta_K$ is the discriminant of $K$. Since then, the class group has taken a prominent role in number theory, but it still remains a rather mysterious object.

From a heuristic standpoint, the class group is better understood in families of number fields due to the conjectures of Cohen and Lenstra [12] and later Cohen and Martinet [13]. The Cohen–Martinet heuristics have several known flaws, and they have been corrected and extended by several authors [8, 28, 34]. To state the Cohen–Lenstra conjectures, let $p$ be an odd prime and let $A$ be a finite, abelian $p$-group. Then the $p$-part of the class group of an imaginary quadratic field is conjectured to be isomorphic to $A$ with probability proportional to $1/\#\mathrm{Aut}(A)$.

For $p = 2$ this obviously breaks down, due to the rather predictable nature of $\mathrm{Cl}(K)[2]$. A natural workaround was found by Gerth, who predicted that a finite abelian 2-group $A$ is

isomorphic to $2\mathrm{Cl}(K)[2^\infty]$ with probability proportional to $1/\#\mathrm{Aut}(A)$. This was recently proven by Smith [31]. The odd part remains a mystery, with the most significant result due to Davenport and Heilbronn [14] on the first moment, which was later independently improved by Bhargava, Shankar and Tsimerman [10] and Taniguchi and Thorne [32]. There are also results on class groups of cubic fields [9, 11] and $S_n$-fields [22].

In this paper we are precisely interested in the case where the degree of the number field is not coprime to the part of the class group we are studying. This case is excluded in the heuristics of Cohen and Lenstra and of Cohen and Martinet, and we hope that this work will aid in the development of heuristics in this case. Other known results regarding statistical properties of class groups in families where the degree is not coprime to the part of the class group are due to Fouvry and Klüners [16, 17, 18, 19], Klys [24], Koymans and Pagano [25] and Pagano and Sofos [30], who developed heuristics for ray class groups based on work of Varma [33] and proved them for the 4-rank of imaginary quadratic fields.

To state the main result, we use the following notations. For $\ell \in \{1,3\}$ and $n \geq 1$ an integer, let $\omega_\ell(n)$ be the number of distinct prime factors of $n$ which are congruent to $\ell$ modulo 4. We define $K_n := \mathbb{Q}(i, \sqrt{n})$ and we let $\mathrm{Cl}(K_n)$ be the class group of $K_n$. These fields were first studied by Dirichlet, in the context of quadratic forms [15], and further studied for special values of $n$ by Azizi et al. (see, e.g., [2, 1, 3, 4, 5, 6, 7], and also [20]). Furthermore, the $2^k$-rank of a finite abelian group $A$ is by definition $\mathrm{rk}_{2^k} A := \dim_{\mathbb{F}_2} 2^{k-1}A/2^k A$.

**Theorem 1.1.** *Uniformly for $x \geq 2$, we have*

$$\#\{0 < n < x : n \text{ odd and square free, } \mathrm{rk}_4\mathrm{Cl}(K_n) \neq \omega_3(n) - 1\} = O\left(\frac{x}{(\log x)^{1/8}}\right).$$

In simple terms, we have that the 4-rank of $\mathrm{Cl}(K_n)$ is $\omega_3(n) - 1$ for 100% of the odd, square free integers $n$. Note that this behavior is wildly different from the case of quadratic extensions of $\mathbb{Q}$ (see [20, Proposition 12], for instance), and we believe it to be a nontrivial task to develop appropriate heuristics in this setting. A weaker result can be found in [20, Theorem 1], where it is proven that at least 28% of the odd, square free integers $n$ satisfy $\mathrm{rk}_4\mathrm{Cl}(K_n) = \omega_3(n) - 1$.

To prove Theorem 1.1, we start by giving a description of $\mathrm{Cl}(K_n)^\vee[2]$. Such a description can be obtained from the work of Fröhlich [21], who studied $\mathrm{Cl}(K)^\vee[2]$ for any biquadratic extension $K$ of $\mathbb{Q}$. This was later extended to $\mathrm{Cl}(K)^\vee[2]$ with $K$ an arbitrary multiquadratic extension of $\mathbb{Q}$ in [26].

Once we have described $\mathrm{Cl}(K_n)^\vee[2]$, we are in the position to obtain a criterion for an element of $\mathrm{Cl}(K_n)^\vee[2]$ to be in $2\mathrm{Cl}(K_n)^\vee[4]$. To do so, we introduce the notion of genericity.

**Definition 1.2.** We say that an odd, square free integer $n > 0$ is *generic* if it has a prime divisor 5 modulo 8.

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

This notion of a generic integer already appears in [20]. More precisely, for $n$ odd and square free (see [20, Proposition 8]), we have

$$\mathrm{rk}_2(\mathrm{Cl}(K_n)) = \begin{cases} 2\omega_1(n)+\omega_3(n)-1 \text{ if } n \text{ is generic,} \\ 2\omega_1(n)+\omega_3(n)-2 \text{ if } n \text{ is not generic.} \end{cases}$$

As we shall see, our algebraic criterion is only valid if $n$ is generic. It is here that we make essential use of the fact that $\mathbb{Q}(i)$ has class number 1, and it is plausible that Theorem 1.1 can be extended to any family of the shape $\mathbb{Q}(\sqrt{d},\sqrt{n})$ as long as $d$ is negative and $\mathbb{Q}(\sqrt{d})$ has class number 1. It would be most interesting to extend the results further to the case that $\mathbb{Q}(\sqrt{d})$ does not have class number 1.

We shall reserve the letter $\pi$ for irreducible elements in $\mathbb{Z}[i]$. For $n \geq 3$ an odd, square free integer, we introduce the following arithmetical function $f(n)$:

$$f(n) := \frac{1}{4} \cdot \sharp\Big\{\beta \in \mathbb{Z}[i] : \ \beta \equiv \pm 1 \bmod 4\mathbb{Z}[i],\ \beta | n \text{ such that} \\ \text{for all } \pi|\beta, \text{ the Gaussian integer } n/\beta \text{ is a square modulo } \pi, \\ \text{and for all } \pi|(n/\beta), \text{ the Gaussian integer } \beta \text{ is a square modulo } \pi\Big\}. \quad (1.1)$$

This function resembles the quantity appearing in [16, Lemma 16]. The definition of $f(n)$ directly implies that it is a power of 2 satisfying the inequalities

$$1 \leq f(n) \leq 2^{2\omega_1(n)+\omega_3(n)-1}.$$

We can now state our key algebraic result.

**Theorem 1.3.** *Let $n$ be generic. Then we have*

$$2^{\mathrm{rk}_4\mathrm{Cl}(K_n)} = f(n),$$

*and furthermore, $f(n) \geq 2^{\omega_3(n)-1}$.*

With the aid of Magma we computed a list of generic integers $3 \leq n \leq 1000$ for which $\mathrm{rk}_4\mathrm{Cl}(K_n) \geq \omega_3(n)$. By Theorem 1.3 we certainly have for such $n$ that $\mathrm{rk}_4\mathrm{Cl}(K_n) \geq \omega_3(n)-1$. This gives the following table (we have excluded those with $\omega_3(n)=0$, since they trivially satisfy $\mathrm{rk}_4\mathrm{Cl}(K_n) \geq \omega_3(n)$).

| $\omega_3(n)$ | Generic $3 \leq n \leq 1000$ with $\mathrm{rk}_4\mathrm{Cl}(K_n) \geq \omega_3(n)$ |
|---|---|
| 1 | {39, 55, 95, 111, 155, 183, 203, 259, 295, 299, 327, 355, 371, 395, 407, 471, 543, 559, 583, 655, 663, 667, 687, 695, 755, 763, 831, 895, 915, 955, 995} |
| 2 | {777, 897} |

The table shows 33 integers, whereas the total number of generic integers satisfying $3 \leq n \leq 1000$ and $\omega_3(n) > 0$ is 96, of which 78 have $\omega_3(n)=1$ and 18 have $\omega_3(n)=2$. Furthermore, the smallest generic $n$ with $\omega_3(n) > 0$ and $\mathrm{rk}_4\mathrm{Cl}(K_n) \geq \omega_3(n)+1$ is $n=1443$, and the smallest $n$ with instead $\mathrm{rk}_4\mathrm{Cl}(K_n) \geq \omega_3(n)+2$ is $n=4895$.

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

It is not hard to show from our methods that we always have the inequalities

$$2^{\omega_3(n)-2} \leq \frac{f(n)}{2} \leq 2^{\mathrm{rk}_4 \mathrm{Cl}(K_n)} \leq f(n) \tag{1.2}$$

for odd, square free $n \geq 3$. Since our focus is Theorem 1.1, we shall not include the proofs of these inequalities. Our main analytic result shows that, for a special type of averaging, $f(n)$ is close to $2^{\omega_3(n)-1}$. We have the following:

**Theorem 1.4.** *Uniformly for $x \geq 2$, we have*

$$\sum_{n \leq x} \mu^2(2n) \Big( \frac{f(n)}{2^{\omega_3(n)-1}} \Big) = \sum_{n \leq x} \mu^2(2n) + O(x \log^{-1/8} x). \tag{1.3}$$

Standard methods from analytic number theory show the equality

$$\sum_{n \leq x} \mu^2(2n) = \frac{4}{\pi^2} \cdot x + O(\sqrt{x}), \tag{1.4}$$

uniformly for $x \geq 2$. This shows that (1.3) is an asymptotic formula.

With slightly more effort, particularly in the proof of Lemma 8.2, it is possible to improve the error term in (1.3) to $O(x \log^{-\theta} x)$ for any $\theta < 1/4$. The equality (1.3) could be generalised to the set of integers $n \leq x$ such that all the prime divisors of $n$ belong to an imposed congruence class.

The layout of the paper is as follows. In §2 we study the 2-torsion of $\mathrm{Cl}(K_n)$. Then in §3 we derive our pivotal algebraic results, culminating in the proof of Theorem 1.3. The next sections are devoted to the analysis of the sum appearing in (1.3). Finally, in §10 we show how Theorems 1.3 and 1.4 imply Theorem 1.1.

## 2. On the 2-torsion of $\mathrm{Cl}(K_n)$

For an abelian group $A$, we write $A[m]$ for the part of $A$ that is killed by $m$ and $A^\vee := \mathrm{Hom}(A, \mathbb{C})$ for its dual. We denote the set $\{1, \dots, n\}$ by $[n]$. In what follows, we let $n \in \mathbb{Z}_{\geq 3}$ be an odd, square free integer. Recall that $n$ is *generic* in case there exists a prime number congruent to 5 modulo 8 that divides $n$. Write $n := p_1 \cdot \ldots \cdot p_r \cdot q_1 \cdot \ldots \cdot q_s$, where for each $(h, k) \in [r] \times [s]$ we have that $p_h$ and $q_k$ are respectively 1 and 3 modulo 4. For each $h \in [r]$, decompose $p_h$ in $\mathbb{Z}[i]$ as

$$p_h := \pi_h \cdot \overline{\pi_h},$$

where $\pi_h := a_h + i b_h$ with $2 \mid b_h$ and $a_h \equiv 1 \bmod 4$. The following gives a complete description of the quadratic extensions of $K_n$ that are unramified at all finite places – and thus, since $K_n$ is totally complex, a description of the space $\mathrm{Cl}(K_n)^\vee[2]$ by class field theory.

**Proposition 2.1.** *Let $L/K_n$ be a quadratic extension. Then it is unramified if and only if there exist functions*

$$\epsilon_1, \epsilon_2 : [r] \to \{0, 1\}, \alpha : [s] \to \{0, 1\}$$

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

*such that*

$$\sum_{h\in[r]:p_h\equiv 5 \bmod 8} \Big(\epsilon_1(h)+\epsilon_2(h)\Big) \equiv 0 \bmod 2 \tag{2.1}$$

*and*

$$L=\mathbb{Q}\left(i,\sqrt{n},\sqrt{\prod_{h\in[r]}\pi_h^{\epsilon_1(h)}\overline{\pi_h}^{\epsilon_2(h)}\cdot\prod_{k\in[s]}q_k^{\alpha(k)}}\right).$$

**Proof.** It is well known that $\mathbb{Z}[i]$ is a principal ideal domain. It follows that the generator of $\mathrm{Gal}(K_n/\mathbb{Q}(i))$ acts as $-\mathrm{id}$ on $\mathrm{Cl}(K_n)$. In particular, every unramified abelian extension of $K_n$ remains Galois over $\mathbb{Q}(i)$. Furthermore, we know that the extension $K_n/\mathbb{Q}(i)$ must ramify at some finite place $v$ of $\mathbb{Q}(i)$. Hence an inertia group at $v$ in $\mathrm{Gal}(L/\mathbb{Q}(i))$ must be of order 2 and project nontrivially in $\mathrm{Gal}(K_n/\mathbb{Q}(i))$. It follows that $L/\mathbb{Q}(i)$ is a biquadratic extension; in other words, there must be $\gamma\in\mathbb{Q}(i)^*$, with $L=K_n(\sqrt{\gamma})$.

Next we claim that if we have a finite place $v$ of $\mathbb{Q}(i)$ with $v(\gamma)$ odd, then it must be the case that $v(n)>0$. Indeed, $K_n/\mathbb{Q}(i)$ is unramified at all places $v$ with $v(n)=0$; observe that this is also correct at $1+i$, since $n$ is a rational integer. But $\mathbb{Q}(i,\sqrt{\gamma})/\mathbb{Q}(i)$ will certainly ramify at $v$ in case $v(\gamma)$ is odd, and hence the extension $K_n(\sqrt{\gamma})/K_n$ will ramify at any place of $K_n$ above $v$. This shows our claim.

Thanks to the last step, and since $\mathbb{Z}[i]$ is a principal ideal domain, we can suppose that $\gamma$ is an element of $\mathbb{Z}[i]$ that divides $n$ in $\mathbb{Z}[i]$.

Now let $a+ib$ be an element of $\mathbb{Z}[i]$, with $a\not\equiv b \bmod 2$ – that is, $a+ib$ is coprime to $1+i$. Then we claim that $\mathbb{Q}(i,\sqrt{a+ib})$ is unramified at $1+i$ if and only if $4\mid b$. To this end, we recall that elements of $\mathbb{Z}_2[i]$ of the shape $1+(1+i)u$ or $1+(1+i)^3u$, with $u\in\mathbb{Z}_2[i]^*$, yield ramified quadratic extensions of $\mathbb{Q}_2(i)$. We first show that $2\mid b$. Suppose not. Then, by our assumption on $a+ib$, it must be that $a$ is even. Then we can rewrite $a+ib=2a'+2ib'+i=2(a'+ib')+i$ with $a',b'$ integers. This can be rewritten as $1+(1+i)u$ with $u\in\mathbb{Z}_2[i]^*$.

So we must have that $2\mid b$ and $a\equiv 1 \bmod 2$. Furthermore, since $-1$ is a square in $\mathbb{Q}(i)$, we can assume that $a$ is 3 modulo 4. Now suppose that 4 does not divide $b$. Then we can rewrite $a+ib=a+2ib'=-1+4a'+2ib'$, where $a',b'$ are integers and $b'$ is odd, which equals $-1+2i+4z=1-2(1-i)+4z$ with $z\in\mathbb{Z}[i]$. This has the shape $1+(1+i)^3u$, with $u$ a unit in $\mathbb{Z}_2[i]$. Therefore it yields a ramified extension of $\mathbb{Q}_2(i)$ and the desired claim is proved.

We have obtained that $\gamma=a+ib$ is a divisor of $n$ with $a$ odd and $b$ divisible by 4. Observe furthermore that since $-1$ is a square in $\mathbb{Q}(i)$, we can reduce to the case that $a$ is 1 modulo 4. Now it is straightforward to check that $\gamma$ is precisely one of the elements listed previously. Conversely, it is easy to check that all such $\gamma$ give an unramified extension. □

We denote by $\mathrm{Gn}(K_n)$ the span of the elements listed in Proposition 2.1 in $\frac{\mathbb{Q}(i)^*}{\mathbb{Q}(i)^{*2}}$. More precisely, these are the elements

$$\prod_{h\in[r]}\pi_h^{\epsilon_1(h)}\overline{\pi_h}^{\epsilon_2(h)}\cdot\prod_{k\in[s]}q_k^{\alpha(k)},$$

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

as $\epsilon_1, \epsilon_2 : [r] \to \{0,1\}, \alpha : [s] \to \{0,1\}$ varies and satisfies (2.1).

## 3. A criterion for the 4-torsion for generic $n$

We shall now establish a general fact that will be the key tool to exploit the condition of genericity on $n$. To do so, we start by recalling the inflation–restriction exact sequence. Let $G$ be a profinite group, $N$ a normal open subgroup and $A$ a discrete $G$-module. Note that $G/N$ naturally acts on $A^N$. Then we have an exact sequence

$$0 \to H^1(G/N, A^N) \to H^1(G, A) \to H^1(N, A)^{G/N} \to H^2(G/N, A^N) \to H^2(G, A), \quad (3.1)$$

where the second and fifth maps are inflation, the third map is restriction and the fourth map is transgression. We remark that $G$ naturally acts on $H^1(N, A)$ by sending a cocycle $f : N \to A$ to $(g \cdot f)(n) = g \cdot f(g^{-1}ng)$, and this action descends to an action of $G/N$.

For a field $K$, we denote by $G_K$ the absolute Galois group of $K$. If $L/K$ is any finite Galois extension of fields of characteristic different from 2, we apply the inflation–restriction sequence with $G = G_K$, $N = G_L$ and $A = \mathbb{F}_2$ with trivial action. There is, by Kummer theory, an isomorphism

$$H^1(N, A)^{G/N} \cong \left(\frac{L^*}{L^{*2}}\right)^{\mathrm{Gal}(L/K)}.$$

The map from right to left is given by sending $\alpha$ to the character $\chi_\alpha$, which is by definition the character corresponding to $\sqrt{\alpha}$. Combining this with the inflation–restriction exact sequence, we obtain a natural map

$$r : \left(\frac{L^*}{L^{*2}}\right)^{\mathrm{Gal}(L/K)} \to H^2(\mathrm{Gal}(L/K), \mathbb{F}_2),$$

whose kernel consists precisely of the image of $K^*$ in $L^*/L^{*2}$ and whose image consists precisely of those classes in $H^2(\mathrm{Gal}(L/K), \mathbb{F}_2)$ that become trivial when inflated to $H^2(G_K, \mathbb{F}_2)$. We start with a lemma.

**Lemma 3.1.** *Let $E$ be a local field of characteristic 0 and let $F/E$ be an unramified extension. Then the inflation map*

$$H^2(\mathrm{Gal}(F/E), \mathbb{F}_2) \to H^2(G_E, \mathbb{F}_2)$$

*is the zero map.*

**Proof.** This is a special case of [25, Proposition 4.4]. □

We can now prove the following proposition, which is based on ideas from [26, Proposition 4.10]. We say that a class $\theta \in H^2(\mathrm{Gal}(L/\mathbb{Q}(i)), \mathbb{F}_2)$ is *locally trivial* at a place $v$ of $\mathbb{Q}(i)$ if $\theta$ is trivial in $H^2(G_{\mathbb{Q}(i)_v}, \mathbb{F}_2)$.

**Proposition 3.2.** *Let $L/\mathbb{Q}(i)$ be a Galois 2-extension of $\mathbb{Q}(i)$ and take $p$ to be a rational prime that is congruent to 5 modulo 8. Suppose that $L$ ramifies at both places of $\mathbb{Q}(i)$ lying above $p$. Assume that $1+i$ is unramified in $L/\mathbb{Q}(i)$. Let $\theta \in H^2(\mathrm{Gal}(L/\mathbb{Q}(i)), \mathbb{F}_2)$ be such that the inflation of $\theta$ to $G_{\mathbb{Q}(i)}$ is locally trivial at all the places of $\mathbb{Q}(i)$ which ramify*

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

*in $L/\mathbb{Q}(i)$. Suppose furthermore that for each odd place $v$ of $\mathbb{Q}(i)$, the class $\theta$ restricted to an inertia subgroup $I_v$ of $\mathrm{Gal}(L/\mathbb{Q}(i))$ yields a trivial element of $H^2(I_v, \mathbb{F}_2)$.*

*Then there exists $\alpha \in \left(\frac{L^*}{L^{*2}}\right)^{\mathrm{Gal}(L/\mathbb{Q}(i))}$ with $r(\alpha) = \theta$ and $L(\sqrt{\alpha})/L$ unramified.*

**Proof.** We first claim that there exists $\alpha$ such that $r(\alpha) = \theta$ and the extension $L(\sqrt{\alpha})/L$ is unramified above any odd place. Consider the exact sequence

$$1 \to \{\pm 1\} \to \overline{\mathbb{Q}(i)}^* \to \overline{\mathbb{Q}(i)}^* \to 1,$$

where the map from $\overline{\mathbb{Q}(i)}^*$ to $\overline{\mathbb{Q}(i)}^*$ is squaring. Taking Galois cohomology and using Hilbert Theorem 90, we deduce that there is an injection

$$0 \to H^2(G_{\mathbb{Q}(i)}, \mathbb{F}_2) \to H^2(G_{\mathbb{Q}(i)}, \overline{\mathbb{Q}(i)}^*).$$

Then by class field theory, we have another injection

$$0 \to H^2(G_{\mathbb{Q}(i)}, \overline{\mathbb{Q}(i)}^*) \to \bigoplus_{v \in \Omega_{\mathbb{Q}(i)}} H^2(G_{\mathbb{Q}(i)_v}, \overline{\mathbb{Q}(i)_v}^*),$$

where $\Omega_{\mathbb{Q}(i)}$ are the places of $\mathbb{Q}(i)$. Hence, to check if $\theta$ is trivial in $H^2(G_{\mathbb{Q}(i)}, \mathbb{F}_2)$, we can check this locally in $H^2(G_{\mathbb{Q}(i)_v}, \overline{\mathbb{Q}(i)_v}^*)$ for every $v \in \Omega_{\mathbb{Q}(i)}$. By assumption, $\theta$ is trivial locally at all places $v$ that ramify in $L/\mathbb{Q}(i)$. Furthermore, Lemma 3.1 shows that $\theta$ is trivial at the unramified places, and hence we have shown that $\theta$ is trivial in $H^2(G_{\mathbb{Q}(i)}, \mathbb{F}_2)$. We deduce that there is $\alpha$ with $r(\alpha) = \theta$.

Our next task is to adjust $\alpha$ with elements in $\mathbb{Q}(i)^*$ such that $L(\sqrt{\alpha})/L$ is unramified at the odd places. Suppose that $L(\sqrt{\alpha})/L$ is ramified at some odd place $w$ of $L$. If $v$ is the place of $\mathbb{Q}(i)$ below $w$, and $v$ is unramified in $L/\mathbb{Q}(i)$, then we twist $\alpha$ by $\pi$, with $\pi$ a prime element of $\mathbb{Z}[i]$ corresponding to $v$. Since $\alpha$ is invariant modulo squares, this ensures that $v$ is unramified in $L(\sqrt{\alpha\pi})/L$ without changing the ramification at any other odd place.

Now suppose instead that the place $v$ below $w$ is ramified in $L/\mathbb{Q}(i)$. We filter $L_w/\mathbb{Q}(i)_v$ as a tower $L_w/K/\mathbb{Q}(i)_v$, where $K$ is the largest unramified extension of $\mathbb{Q}(i)_v$ inside $L_w$. The assumption that $\theta$ is trivial when restricted to $I_v$ precisely implies, by the inflation–restriction sequence in (3.1), that $\chi_\alpha$ equals the restriction of some central character $\chi$ from $G_K$. Since $v$ is an odd place, such characters are in the span of the unramified character of $K$ and a ramified character of $\mathbb{Q}(i)_v$. Therefore the extension $L(\sqrt{\alpha})/L$ is automatically unramified at $v$ for any choice of $\alpha$ with $r(\alpha) = \theta$.

Having established the claim, it remains to adjust the ramification at $1+i$. Let $w$ be a place of $L$ above $1+i$. By assumption, $L_w/\mathbb{Q}_2(i)$ is unramified. Therefore the Galois group $\mathrm{Gal}(L_w/\mathbb{Q}_2(i))$ is cyclic and thus $H^2(\mathrm{Gal}(L_w/\mathbb{Q}_2(i)), \mathbb{F}_2)$ is cyclic of order 2. The nontrivial element in $H^2(\mathrm{Gal}(L_w/\mathbb{Q}_2(i)), \mathbb{F}_2)$ is realised via an unramified extension. Hence there exists $c \in \mathbb{Q}(i)^*$ such that $c\alpha$ yields an unramified class of $\frac{L_w^*}{L_w^{*2}}$ for all choices of $w$ above $v$. Furthermore, since $\alpha$ is invariant modulo squares, the same $c$ will work simultaneously for all places $w$ of $L$ above $1+i$.

Now let $p = \pi\overline{\pi}$ be a factorisation of our prime $p \equiv 5 \bmod 8$ in $\mathbb{Z}[i]$. Observe that multiplying $\alpha$ by elements in the span of $\{\pi, \overline{\pi}, i, 1+i\}$ changes only the ramification at the places above 2. Indeed, this follows from the assumption that $\theta$ is trivial when

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

restricted to $H^2(I_v,\mathbb{F}_2)$. Now $p\equiv 5 \bmod 8$ implies that $\{\pi,\overline{\pi},i,1+i\}$ is a basis of $\frac{\mathbb{Q}_2(i)^*}{\mathbb{Q}_2(i)^{*2}}$. Hence $c$ can be picked in the space $\langle\{\pi,\overline{\pi},i,1+i\}\rangle$, cleaning the ramification precisely at the places above $1+i$ without affecting any other place of $L$, which concludes our proof. □

Let $n\in\mathbb{Z}_{\geq 3}$ be odd, square free and generic. We can now describe the space $2\mathrm{Cl}(K_n)^\vee[4]$. For any place $v$ of $\mathbb{Q}(i)$, we denote by $(-,-)_v$ the Hilbert symbol pairing defined on $\mathbb{Q}(i)_v^*$ and attaining values in $\{1,-1\}$. Recall that for $x,y\in\mathbb{Q}(i)_v^*$, we have that $(x,y)_v=1$ if and only if $\chi_x\cup\chi_y$ yields a trivial class in $H^2(G_{\mathbb{Q}(i)_v},\mathbb{F}_2)$.

**Proposition 3.3.** *Let $n\in\mathbb{Z}_{\geq 3}$ be odd, square free and generic. Let $\alpha$ be in $\mathrm{Gn}(K_n)$. Then the character $\chi_\alpha$ is in $2\mathrm{Cl}(K_n)^\vee[4]$ if and only if for any finite place $v$ with $v(n)\neq 0$,*

$$\left(\alpha,\frac{n}{\alpha}\right)_v=1.$$

**Remark 1.** The forward implication will not use the fact that $n$ is generic, but for the other implication this will be crucial.

**Proof.** Observe that the elements $\alpha$ in $\mathrm{Gn}(K_n)$ with $\chi_\alpha\in 2\mathrm{Cl}(K_n)^\vee[4]$ are, if nontrivial, precisely those with $K_n(\sqrt{\alpha})$ contained in a cyclic degree 4 unramified extension of $K_n$. Such an extension is Galois over $\mathbb{Q}(i)$, as we argued in Proposition 2.1. Furthermore, picking an inertia element at a place dividing $\alpha$ and one at a place dividing $\frac{n}{\alpha}$ gives a lift by involutions of the basis of $\mathrm{Gal}(K_n(\sqrt{\alpha})/\mathbb{Q}(i))$ dual to $\{\chi_\alpha,\chi_{\frac{n}{\alpha}}\}$. This forces $L$ to be $K_n(\sqrt{\alpha},\sqrt{\beta})$, with

$$\beta\in\left(\frac{K_n(\sqrt{\alpha})^*}{K_n(\sqrt{\alpha})^{*2}}\right)^{\mathrm{Gal}(K_n(\sqrt{\alpha})/\mathbb{Q}(i))}$$

and

$$r(\beta)=\chi_\alpha\cup\chi_{\frac{n}{\alpha}}.$$

Conversely, any time we realise – via the map $r$ – this class via an unramified quadratic extension of $K_n(\sqrt{\alpha})$, we conclude that $\chi_\alpha\in 2\mathrm{Cl}(K_n)^\vee[4]$.

Hence, for the 'only if' part, we see that $\chi_\alpha\cup\chi_{\frac{n}{\alpha}}$ must be in the image of $r$. It follows that $\chi_\alpha\cup\chi_{\frac{n}{\alpha}}$ is in the kernel of the inflation to $H^2(G_{\mathbb{Q}(i)},\mathbb{F}_2)$ by the inflation–restriction exact sequence (see (3.1)). But then $\chi_\alpha\cup\chi_{\frac{n}{\alpha}}$ must be locally trivial at all places $v$, and this implies precisely that $\left(\alpha,\frac{n}{\alpha}\right)_v=1$ for all finite places $v$ with $v(n)\neq 0$.

For the 'if' part, we apply Proposition 3.2 with $\theta:=\chi_\alpha\cup\chi_{\frac{n}{\alpha}}$. Since $\left(\alpha,\frac{n}{\alpha}\right)_v=1$ for all finite places $v$ with $v(n)\neq 0$ by assumption, we see that $\theta$ is locally trivial at all places of $\mathbb{Q}(i)$ that ramify in $L:=K_n(\sqrt{\alpha})$. Furthermore, the shape of $\theta$ shows that the class $\theta$ restricted to an inertia subgroup $I_v$ of $\mathrm{Gal}(L/\mathbb{Q}(i))$ yields a trivial element of $H^2(I_v,\mathbb{F}_2)$ for each odd place $v$ of $\mathbb{Q}(i)$.

The fact that $n$ is generic ensures that we have a prime $p\equiv 5 \bmod 8$ to which we can apply Proposition 3.2. Then Proposition 3.2 gives us the required $\beta$. □

**Corollary 3.4.** *Suppose that $n\geq 3$ is odd, square free and generic. Then we have*

$$\dim_{\mathbb{F}_2} 2\mathrm{Cl}(K_n)^\vee[4]\geq\omega_3(n)-1.$$

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

**Proof.** First of all, we have

$$\dim_{\mathbb{F}_2} \mathrm{Cl}(K_n)^\vee[2] = 2\omega_1(n) + \omega_3(n) - 2$$

by Proposition 2.1 or [20, Proposition 8]. We now consider the linear map $T : \mathrm{Cl}(K_n)^\vee[2] \to \{1,-1\}^{\{v|n\}}$ that sends $\chi_\alpha$ to $\left\{\left(\alpha, \frac{n}{\alpha}\right)_v\right\}_v$, where $v$ runs through all finite places dividing $n$. If $v$ corresponds to a prime $p \equiv 3 \bmod 4$ in $\mathbb{Z}$ and $\alpha \in \mathbb{Z}$, then we have

$$\left(\alpha, \frac{n}{\alpha}\right)_p = (\alpha, n)_p = 1.$$

Combining this with Hilbert reciprocity, we see that the image of $T$ has dimension at most $2\omega_1(n) - 1$. But for generic $n$, the kernel of $T$ is precisely $2\mathrm{Cl}(K_n)^\vee[4]$, by Proposition 3.3. Hence the lemma follows from the rank–nullity theorem. □

We can now prove Theorem 1.3.

**Proof of Theorem 1.3.** Take $n > 0$ to be odd and square free. There is a natural surjective map

$$\{\beta \in \mathbb{Z}[i] : \beta \equiv \pm 1 \bmod 4\mathbb{Z}[i], \beta \mid n\} \to \mathrm{Gn}(K_n).$$

The kernel is given by $-1$ and is hence of size 2. There is also a natural map $\mathrm{Gn}(K_n) \to \mathrm{Cl}(K_n)^\vee[2]$, given by sending $\beta$ to $\chi_\beta$, with kernel given by $\chi_n$, again of size 2. By Proposition 3.3 it follows that for generic $n$,

$$2^{\mathrm{rk}_4 \mathrm{Cl}(K_n)} = \frac{1}{2}\left|\left\{\alpha \in \mathrm{Gn}(K_n) : \left(\alpha, \frac{n}{\alpha}\right)_v = 1 \text{ for all } v\right\}\right|.$$

The condition that $(\alpha, n/\alpha)_v = 1$ for all $v$ is equivalent to the condition that for every $\pi \mid \alpha$, we have that $n/\alpha$ is a square modulo $\pi$, and for every $\pi \mid n/\alpha$, we have that $\alpha$ is a square modulo $\pi$. This shows that

$$2^{\mathrm{rk}_4 \mathrm{Cl}(K_n)} = f(n).$$

The theorem then follows from Corollary 3.4. □

**Remark 2.** It is now easy to prove two of the three inequalities in (1.2). The bound $2^{\mathrm{rk}_4 \mathrm{Cl}(K_n)} \leq f(n)$ follows from Proposition 3.3 and Remark 1. Furthermore, the proof of Corollary 3.4 shows that

$$f(n) \geq 2^{\omega_3(n)-1}$$

without any assumptions on $n$. The final inequality

$$\frac{f(n)}{2} \leq 2^{\mathrm{rk}_4 \mathrm{Cl}(K_n)}$$

is substantially trickier, and we shall only sketch it. From the material here, we see that if $\alpha \in \mathrm{Gn}(K_n)$ is such that $(\alpha, n/\alpha)_v = 1$ for all $v$, then we can pick a nontrivial point on the conic

$$x^2 = \alpha y^2 + \frac{n}{\alpha} z^2$$

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

such that the extension $\mathbb{Q}(i,\sqrt{n},\sqrt{\alpha},\sqrt{x+\sqrt{\alpha}\,y})/\mathbb{Q}(i,\sqrt{n},\sqrt{\alpha})$ is only ramified at 2. Then some local considerations at 2 finish the proof.

## 4. Convention, definitions and classical lemmas

We now pass to the proof of Theorem 1.4.

### 4.1. Gaussian integers

We will follow several conventions that appear in [23, Chapters 9.7 and 9.8] concerning the ring $\mathbb{Z}[i]$ of Gaussian integers. The multiplicative group of its *units* is denoted by $\mathbb{U} := \{\pm 1, \pm i\}$. A Gaussian integer $\alpha$ is said to be *odd* if its norm $\mathrm{N}(\alpha) := \mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha)$ is odd. This condition holds if and only if $1+i$ does not divide $\alpha$. We say that a Gaussian integer $\alpha$ is *primary* if it satisfies the condition

$$\alpha \equiv 1 \bmod 2(1+i).$$

A primary element is necessarily odd. For any odd Gaussian integer $\alpha$, the set of its associates $\{\pm\alpha, \pm i\alpha\}$ contains exactly one primary element. A Gaussian integer $z = x+iy$ with $x$ and $y$ in $\mathbb{Z}$ is said to be *primitive* if the integers $x$ and $y$ are coprime.

An element of the set $\mathcal{P}^{\mathrm{odd}} := \{3,5,7,11,\dots\}$ is called an *odd natural prime*. We denote by $\mathcal{P}^{\mathrm{G}}$ the set of the odd primary irreducible Gaussian integers. A Gaussian integer $z$ belongs to $\mathcal{P}^{\mathrm{G}}$ if and only if it satisfies exactly one of the following two conditions:

- $-z$ belongs to $\mathcal{P}^{\mathrm{odd}}$ and $z$ is congruent to 3 mod 4.
- $z$ is primary and $z\overline{z}$ belongs to $\mathcal{P}^{\mathrm{odd}}$ and is congruent to 1 mod 4.

Any odd Gaussian integer $z$ is the product of a unit and elements of $\mathcal{P}^{\mathrm{G}}$. This decomposition is unique up to the order. When $z$ is primary, this unit is equal to 1. The number of distinct elements of $\mathcal{P}^{\mathrm{G}}$ appearing in this decomposition is denoted by $\widetilde{\omega}(z)$. In particular, if $n$ is an odd positive integer, we have

$$\widetilde{\omega}(n) = 2\omega_1(n) + \omega_3(n).$$

We now give an easy decomposition of a positive integer which will be useful in §6.1.

**Lemma 4.1.** *Let $n \geq 1$ be an odd, square free integer and let $\beta_0$, $\beta_1$, $\beta_2$ and $\beta_3$ be four Gaussian integers such that*

$$n = \beta_0\beta_1\beta_2\beta_3. \tag{4.1}$$

*Then there exist*

- *units $\eta_0$, $\eta_1$, $\eta_2$ and $\eta_3$,*
- *positive integers $b_0$, $b_1$, $b_2$ and $b_3$,*
- *primitive Gaussian integers $z_{k,\ell}$ with $0 \leq k \neq \ell \leq 3$,*

*such that for $0 \leq k \leq 3$ and $\ell \neq k$, the following properties are true:*

(i) *$\beta_k/b_k$ is a primitive Gaussian integer.*

(ii) *$\beta_k = \eta_k b_k \prod_{\ell \neq k} z_{k,\ell}$.*

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

(iii) $z_{\ell,k} = \overline{z_{k,\ell}}$.

(iv) $z_{k,\ell}$ *is primary.*

(v) $\prod_{0\le k\le 3} \eta_k = 1$.

*Finally, given* $(n, \beta_0, \beta_1, \beta_2, \beta_3)$ *satisfying* (4.1)*, there is a unique set* $\{\eta_k, b_k, z_{k,\ell}\}$ *satisfying these conditions.*

**Remark 3.** In this decomposition, no $z_{k,\ell}$ is divisible by some element of $\mathcal{P}^{\mathrm{odd}}$. The elements of the set $\{b_k, z_{k,\ell}\}$ are coprime in pairs, since $n$ is square free. To lighten some notations, we will write $z_{k\ell}$ instead of $z_{k,\ell}$. Note that condition (v) follows from the other conditions.

### 4.2. Sums of multiplicative functions

We introduce the notation

$$\mathcal{L} := \log 2x.$$

When bounding several error terms trivially, we will frequently use the following lemma:

**Lemma 4.2.** *Let* $\kappa > 0$ *be fixed. Then uniformly for* $x \ge 1$*, the following bounds hold true:*

$$\sum_{n\le x} \mu^2(n)\kappa^{\omega(n)} \ll x\,\mathcal{L}^{\kappa-1},$$

$$\sum_{n\le x} \mu^2(n)\kappa^{\omega(n)} n^{-1} \ll \mathcal{L}^{\kappa},$$

*and for* $\ell = 1$ *or* $3$*,*

$$\sum_{\substack{n\le x\\ p\mid n\Rightarrow p\equiv \ell \bmod 4}} \mu^2(n)\kappa^{\omega(n)} \ll x\,\mathcal{L}^{\kappa/2-1},$$

$$\sum_{\substack{n\le x\\ p\mid n\Rightarrow p\equiv \ell \bmod 4}} \mu^2(n)\kappa^{\omega(n)} n^{-1} \ll \mathcal{L}^{\kappa/2}.$$

**Proof.** Using Rankin's trick, we readily deduce the second and fourth inequalities. The first and third then follow from [29, Theorem 2.14]. □

### 4.3. Characters to detect squares

In definition (1.1) we need to detect whether a Gaussian integer is a square or not modulo a given Gaussian prime $\pi$. This detection will be accomplished by a character which generalises the Legendre symbol to the ring of Gaussian integers. If $\alpha$ is a nonzero Gaussian integer, the number of residue classes of $\mathbb{Z}[i]$ modulo $\alpha\mathbb{Z}[i]$ is $\mathrm{N}(\alpha)$, and $\phi(\alpha)$ is the number of these classes which are coprime with $\alpha$.

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

**Definition 4.3.** Let $\pi$ be an odd irreducible element of $\mathbb{Z}[i]$ and let $\alpha$ be an element of $\mathbb{Z}[i]$. Then we put

$$\left[\frac{\alpha}{\pi}\right] := \begin{cases} 0 & \text{if } \pi \mid \alpha, \\ 1 & \text{if } \pi \nmid \alpha \text{ and } \alpha \text{ is a square mod } \pi, \\ -1 & \text{if } \pi \nmid \alpha \text{ and } \alpha \text{ is not a square mod } \pi. \end{cases}$$

This character is sometimes denoted by $\left(\frac{\alpha}{\pi}\right)_{\mathbb{Q}(i),2}$. It has the important property of being the square of the quartic character $\chi_\pi(\alpha)$, which is for instance defined in [23, p. 122], and it plays a central role in [17, §4]. We extend $[\frac{\cdot}{\cdot}]$ by multiplicativity to odd composite moduli $\beta$ factorised as a product of irreducible elements $\beta = \pi_1 \cdots \pi_s$, by the formula

$$\left[\frac{\alpha}{\beta}\right] = \left[\frac{\alpha}{\pi_1}\right] \cdots \left[\frac{\alpha}{\pi_s}\right],$$

which is the analogue of the Jacobi symbol.

We recall several formulas satisfied by the character $[\frac{\cdot}{\cdot}]$. The letter $\eta$ denotes an element of $\mathbb{U}$, the letter $\alpha$ denotes a Gaussian integer, the letters $\beta$, $\beta_1$, $\beta_2$ denote odd Gaussian integers and $\pi$ is an odd irreducible element of $\mathbb{Z}[i]$. We have

$$\left[\frac{\alpha}{\pi}\right] \equiv \alpha^{\frac{\mathrm{N}(\pi)-1}{2}} \bmod \pi,$$

$$\left[\frac{\alpha}{\eta}\right] = 1, \left[\frac{\alpha}{\eta\beta}\right] = \left[\frac{\alpha}{\beta}\right], \tag{4.2}$$

$$\left[\frac{\alpha_1\alpha_2}{\beta}\right] = \left[\frac{\alpha_1}{\beta}\right] \cdot \left[\frac{\alpha_2}{\beta}\right], \ \left[\frac{\alpha}{\beta_1\beta_2}\right] = \left[\frac{\alpha}{\beta_1}\right] \cdot \left[\frac{\alpha}{\beta_2}\right], \tag{4.3}$$

$$\left[\frac{\alpha+\beta}{\beta}\right] = \left[\frac{\alpha}{\beta}\right],$$

$$\left[\frac{1}{\beta}\right] = \left[\frac{-1}{\beta}\right] = 1, \ \left[\frac{i}{\beta}\right] = \left[\frac{-i}{\beta}\right] = \begin{cases} 1 & \text{if } \mathrm{N}(\beta) \equiv 1 \bmod 8, \\ -1 & \text{if } \mathrm{N}(\beta) \equiv 5 \bmod 8, \end{cases} \tag{4.4}$$

$$\sum_{\alpha \bmod \beta} \left[\frac{\alpha}{\beta}\right] = \begin{cases} 0 & \text{if } \beta \neq \eta\beta_1^2, \\ \phi(\beta) & \text{if } \beta = \eta\beta_1^2, \end{cases}$$

$$\left[\frac{\overline{\alpha}}{\overline{\beta}}\right] = \left[\frac{\alpha}{\beta}\right]. \tag{4.5}$$

If the real parts of $\alpha$ and $\beta$ are odd and $\alpha$ is odd (for instance when $\alpha$ and $\beta$ are primary), we have the *reciprocity formula* due to Gauss (see [27, Proposition 5.1], for instance):

$$\left[\frac{\alpha}{\beta}\right] = \left[\frac{\beta}{\alpha}\right]. \tag{4.6}$$

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

If $n$ belongs to $\mathbb{Z}$ and if $\pi$ is such that $\pi\overline{\pi} = p$ belongs to $\mathcal{P}^{\mathrm{odd}}$, we have

$$\left[\frac{n}{\pi}\right] = \left(\frac{n}{p}\right), \tag{4.7}$$

where the Legendre symbol appears on the right-hand side. If $a$ and $b$ are positive integers, with $(2a, b) = 1$, we have

$$\left[\frac{a}{b}\right] = 1. \tag{4.8}$$

## 5. Oscillations of characters

### 5.1. Siegel–Walfisz–type theorems

**Lemma 5.1.** *For every $A > 0$, we have*

$$\sum_{n\le x} \frac{\mu^2(nr)}{4^{\omega(n)}}\left(\frac{n}{q}\right) = O_A\left(\sqrt{q}\, x\, 2^{\omega(r)}\, \mathcal{L}^{-A}\right),$$

*uniformly over integers $r \ge 1$, $x \ge 2$ and odd, square free integers $q > 1$.*

**Remark 4.** Such a sum is treated in [16, p. 477] (with the constant 4 replaced by 2), but the proof is different: after restricting to integers $n$ with a reasonable number of prime factors, we apply the classical Siegel–Walfisz theorem to the largest prime factor. Such a device also appears in [17, (80)] and in [19, p. 3631].

**Proof.** Consider the arithmetic function

$$a(n) = a_{q,r}(n) := \frac{\mu^2(nr)}{4^{\omega(n)}}\left(\frac{n}{q}\right)$$

and the associated Dirichlet series

$$F(s) := \sum_{n\ge 1} \frac{a(n)}{n^s} = \prod_{p\nmid r}\left(1 + \frac{\left(\frac{p}{q}\right)}{4p^s}\right),$$

considered as a function of the complex variable $s = \sigma + it$. This Dirichlet series is absolutely convergent for $\sigma > 1$. Its expression as an Euler product leads to the formula

$$F(s) = G_r(s)\{L(s, (\cdot/q))\}^{1/4},$$

where the function $G_r(s)$ is holomorphic on the half-plane $\Re s > 9/10$ and satisfies in this region the inequality $G_r(s) = O(2^{\omega(r)})$, and where the determination of $L(s, (\frac{\cdot}{q}))^{1/4}$ is chosen such that it tends to 1 as $s$ is real and tends to $+\infty$. It is well known that there exists a positive $c > 0$ such that $L(s, (\frac{\cdot}{q}))$ has no zero in the region

$$\Omega := \left\{s : \sigma > 1 - \frac{c}{\log(q(|t|+4))}\right\}, \tag{5.1}$$

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

with at most one exception (Siegel's zero, denoted by $\beta_1$) – which, if it exists, is simple and located on the real axis. Furthermore, it satisfies the inequality

$$\beta_1 < 1 - \frac{c(\varepsilon)}{q^{\varepsilon}},$$

where $\varepsilon > 0$ is arbitrary and $c(\varepsilon) > 0$ (see [29, Theorems 11.3 and 11.14], for instance).

We start from the equality

$$\sum_{n \le x} a(n) = \int_{2-i\infty}^{2+i\infty} F(s) x^s \frac{ds}{s}.$$

If there is no Siegel zero $\beta_1$, we shift the contour of integration to the path $\mathcal{G}$ defined by

$$\sigma = 1 - \frac{c/2}{\log(q(|t|+2))},$$

where $c$ is the constant appearing in (5.1). If $\beta_1$ exists, we replace the part of $\mathcal{G}$ satisfying $|t| \le c(\varepsilon)/(2q^{\varepsilon})$ by two horizontal segments with ordinates $\pm c(\varepsilon)/(2q^{\varepsilon})$ and a semicircle with centre $\beta_1$ and radius $c(\varepsilon)/(2q^{\varepsilon})$. In both cases, all the zeroes of $L$ are on the left of $\mathcal{G}$, and the function $F(s)$ is holomorphic on some open subset containing the part of the complex plane situated on the right-hand side of $\mathcal{G}$. To bound $|F(s)|$ on $\mathcal{G}$, we appeal to the bounds [29, (11.6)] or [29, (11.10)] for $L(s, (\frac{\cdot}{q}))$ according to the existence of $\beta_1$ and the situation of $s$ on $\mathcal{G}$, and we complete the proof of Lemma 5.1. This procedure is similar to the proof of the Siegel–Walfisz theorem on sums of values of Dirichlet characters on consecutive primes. □

### 5.2. Double oscillation bounds for Jacobi symbols

Consider the bilinear sum over the Jacobi symbol

$$\Omega(\boldsymbol{\xi}, \boldsymbol{\zeta}, M, N) := \sum_{1 \le m \le M} \sum_{1 \le n \le N} \mu^2(2m)\mu^2(2n)\xi(m)\zeta(n)\Big(\frac{m}{n}\Big),$$

where $\boldsymbol{\xi}$ and $\boldsymbol{\zeta}$ are given sequences of complex numbers. We recall [16, Lemma 15(18)] (see also [18, Proposition 10]).

**Lemma 5.2.** *Let $\xi(m)$ and $\zeta(n)$ be complex sequences with modulus less than 1. Then for every $\varepsilon > 0$, uniformly for $M$ and $N \ge 1$ we have*

$$\Omega(\boldsymbol{\xi}, \boldsymbol{\zeta}, M, N) \ll_{\varepsilon} MN(M^{-1/2+\varepsilon} + N^{-1/2+\varepsilon}). \tag{5.2}$$

This quite general lemma shows cancellation as soon as $\min(M, N)$ tends to infinity. Actually, we will use Lemma 5.2 under an extended form, where the number of divisors of the integer $n$ is denoted by $d(n)$.

**Lemma 5.3.** *Let $\xi(m)$ and $\zeta(n)$ be complex sequences, such that $|\xi(m)| \le d(m)$ and $|\zeta(n)| \le 1$ for all $m$ and $n \ge 1$. Then for every $\varepsilon > 0$, uniformly for $K$, $M$ and $N \ge 1$ we have*

$$\Omega(\boldsymbol{\xi}, \boldsymbol{\zeta}, M, N) \ll_{\varepsilon} KMN(M^{-1/2+\varepsilon} + N^{-1/2+\varepsilon}) + K^{-1}MN(\log M)^3.$$

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

**Proof.** Of course, we could go to the original proof of Lemma 5.2 and insert, for some integer $r$, the $\ell_r$–norm of the sequence $\xi(m)$. We prefer to give a proof starting from Lemma 5.2 itself. We denote by $\Omega_{<K}$ the subsum of $\Omega(\boldsymbol{\xi},\boldsymbol{\zeta},M,N)$ corresponding to pairs $(m,n)$ such that $|\xi(m)|\leq K$ and $\Omega_{\geq K}$ is the complementary sum. So we have $\Omega(\boldsymbol{\xi},\boldsymbol{\zeta},M,N)=\Omega_{<K}+\Omega_{\geq K}$. A direct application of (5.2) gives the bound

$$\Omega_{<K}\ll KMN(M^{-1/2+\varepsilon}+N^{-1/2+\varepsilon}).$$

The other sum, $\Omega_{\geq K}$, is handled trivially by

$$|\Omega_{\geq K}|\leq N\sum_{\substack{m\leq M\\ d(m)\geq K}}d(m)\leq N\sum_{m\leq M}\frac{d(m)^2}{K}\ll K^{-1}MN(\log M)^3.$$

Adding these bounds completes the proof of the lemma. □

### 5.3. Double oscillation bounds for $[\frac{\cdot}{\cdot}]$-symbols

We now consider the situation where, in the bilinear form, the Jacobi symbol is replaced by the $[\frac{\cdot}{\cdot}]$-symbol, which turns out to be very similar.

To be more precise, let us define the bilinear form

$$\Xi(\boldsymbol{\xi},\boldsymbol{\zeta},A,B):=\sum_{\mathrm{N}(\alpha)\leq A}\sum_{\mathrm{N}(\beta)\leq B}\xi(\alpha)\zeta(\beta)\Big[\frac{\alpha}{\beta}\Big],$$

where $\xi(\alpha)$ and $\zeta(\beta)$ are complex numbers defined on the set of odd Gaussian integers $\alpha$ and $\beta$. By a weaker form of [17, Proposition 9], we have the following:

**Lemma 5.4.** *Let $\xi(\alpha)$ and $\zeta(\beta)$ be complex sequences with support included in the set of primary square free Gaussian integers. Furthermore, suppose that these sequences satisfy the inequalities*

$$|\xi(\alpha)|,\ |\zeta(\beta)|\leq 1.$$

*Then uniformly for $A$ and $B\geq 1$, we have*

$$\Xi(\boldsymbol{\xi},\boldsymbol{\beta},A,B)\ll AB(A^{-1/9}+B^{-1/9}).$$

The trivial bound for $\Xi$ is $O(AB)$. Any bound of $\Xi$ of the shape $\Xi\ll AB(A^{-\delta}+B^{-\delta})$ for some positive $\delta$ would be sufficient for the proof of Theorem 1.4. The same remark applies to (5.2).

## 6. Proof of Theorem 1.4: First steps

### 6.1. Transformation of $f(n)$

Our purpose is to use the character $[\frac{\cdot}{\cdot}]$ to transform the function $f(n)$ when $n$ is a positive square free integer. Recall the definition of $f(n)$ (see (1.1)):

$$f(n):=\frac{1}{4}\cdot\sharp\Big\{\beta\in\mathbb{Z}[i]:\ \beta\equiv\pm1 \bmod 4\mathbb{Z}[i],\ \beta|n \text{ such that}$$
$$\text{for all } \pi|\beta,\ \text{the Gaussian integer } n/\beta \text{ is a square modulo } \pi,$$

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

and for all $\pi|(n/\beta)$, the Gaussian integer $\beta$ is a square modulo $\pi$ $\Big\}$.

We further recall that $f(n)$ is equal to $2^{\mathrm{rk}_4\mathrm{Cl}(K_n)}$ for generic $n$, by Theorem 1.3. First of all, the value of $f(n)$ does not change if, in (1.1), we restrict ourselves to primes $\pi$ belonging to $\mathcal{P}^{\mathrm{G}}$. Note that the function

$$\frac{1}{2^{\widetilde{\omega}(\beta)}}\prod_{\substack{\pi|\beta\\ \pi\in\mathcal{P}^{\mathrm{G}}}}\Big(1+\Big[\frac{n/\beta}{\pi}\Big]\Big)=\frac{1}{2^{\widetilde{\omega}(\beta)}}\sum_{\substack{\beta_1|\beta\\ \beta_1\text{ primary}}}\Big[\frac{n/\beta}{\beta_1}\Big] \tag{6.1}$$

detects precisely the condition $\Big[\frac{n/\beta}{\pi}\Big]=1$ *for every* $\pi|\beta$.

Similarly, the function

$$\frac{1}{2^{\widetilde{\omega}(n/\beta)}}\prod_{\substack{\pi|n/\beta\\ \pi\in\mathcal{P}^{\mathrm{G}}}}\Big(1+\Big[\frac{\beta}{\pi}\Big]\Big)=\frac{1}{2^{\widetilde{\omega}(n/\beta)}}\sum_{\substack{\beta_3|n/\beta\\ \beta_3\text{ primary}}}\Big[\frac{\beta}{\beta_3}\Big] \tag{6.2}$$

detects the condition $\Big[\frac{\beta}{\pi}\Big]=1$ *for every* $\pi|n/\beta$. Writing $\beta=\beta_0\beta_1$ and $n/\beta=\beta_2\beta_3$, gathering (6.1) and (6.2) and expanding the sums and the characters, we finally obtain

$$f(n)=\frac{1}{4}\sum_{\beta_0}\frac{1}{2^{\widetilde{\omega}(\beta_0)}}\sum_{\beta_1}\frac{1}{2^{\widetilde{\omega}(\beta_1)}}\sum_{\beta_2}\frac{1}{2^{\widetilde{\omega}(\beta_2)}}\sum_{\beta_3}\frac{1}{2^{\widetilde{\omega}(\beta_3)}}\Big[\frac{\beta_0\beta_1}{\beta_3}\Big]\cdot\Big[\frac{\beta_2\beta_3}{\beta_1}\Big], \tag{6.3}$$

where the sum is over $\boldsymbol{\beta}=(\beta_0,\beta_1,\beta_2,\beta_3)\in\mathbb{Z}[i]^4$ such that

$$n=\beta_0\beta_1\beta_2\beta_3,\ \beta_0\beta_1\equiv\pm1 \bmod 4,\ \beta_1 \text{ and } \beta_3 \text{ primary}. \tag{6.4}$$

These congruence conditions imply that $\beta_1$ and $\beta_3$ both have odd real parts. Hence, by the reciprocity relation (4.6), (6.3) simplifies to

$$f(n)=\frac{1}{4}\sum_{\beta_0}\frac{1}{2^{\widetilde{\omega}(\beta_0)}}\sum_{\beta_1}\frac{1}{2^{\widetilde{\omega}(\beta_1)}}\sum_{\beta_2}\frac{1}{2^{\widetilde{\omega}(\beta_2)}}\sum_{\beta_3}\frac{1}{2^{\widetilde{\omega}(\beta_3)}}\Big[\frac{\beta_0}{\beta_3}\Big]\cdot\Big[\frac{\beta_2}{\beta_1}\Big],$$

where the $\beta_i$ satisfy (6.4). Let

$$S(x):=\sum_{n\leq x}\mu^2(2n)\Big(\frac{f(n)}{2^{\omega_3(n)-1}}\Big)$$

be the sum appearing in (1.3). Inserting the factorisation of the variable $n$ given in (6.4), we obtain

$$S(x)=\frac{1}{2}\sum_{\beta_0}\frac{1}{2^{\widetilde{\omega}(\beta_0)+\omega_3(\beta_0)}}\sum_{\beta_1}\frac{1}{2^{\widetilde{\omega}(\beta_1)+\omega_3(\beta_1)}}\sum_{\beta_2}\frac{1}{2^{\widetilde{\omega}(\beta_2)+\omega_3(\beta_2)}}\sum_{\beta_3}\frac{1}{2^{\widetilde{\omega}(\beta_3)+\omega_3(\beta_3)}}\Big[\frac{\beta_0}{\beta_3}\Big]\cdot\Big[\frac{\beta_2}{\beta_1}\Big], \tag{6.5}$$

where the Gaussian integers $\beta_i$ are odd and satisfy the congruence conditions

$$\beta_0\beta_1\equiv\pm1 \bmod 4,\ \beta_1 \text{ and } \beta_3 \text{ primary}, \tag{6.6}$$

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

the constraint

$$\beta_0\beta_1\beta_2\beta_3 \in \mathbb{N} \text{ and } 1 \le \beta_0\beta_1\beta_2\beta_3 \le x$$

and the coprimality condition

$$(\beta_k, \beta_\ell) = 1 \text{ for } 0 \le k < \ell \le 3.$$

In (6.5) the function $\omega_3$ has naturally been extended to Gaussian integers $z$ by defining $\omega_3(z)$ to be the number of distinct irreducible divisors of $z$ belonging to $\mathcal{P}^{\text{odd}}$.

### 6.2. The main term

Let $S^{\text{MT}}(x)$ be the contribution to the right-hand side of (6.5) coming from $\boldsymbol{\beta} = (\beta_0, \beta_1, \beta_2, \beta_3)$ such that every $\beta_i$ is a nonzero integer, of any sign. When $\beta_i$ are odd integers, (6.6) simply becomes

$$\beta_1 \equiv \beta_3 \equiv 1 \bmod 4. \tag{6.7}$$

When $m$ is a nonzero integer, we have $\widetilde{\omega}(m) + \omega_3(m) = 2\omega(m)$. Then we deduce

$$S^{\text{MT}}(x) = \frac{1}{2} \sum_{1 \le n \le x} \frac{\mu^2(2n)}{4^{\omega(n)}} \cdot \nu(n),$$

where $\nu(n)$ is the number of ways that $n$ can be written as $n = \beta_0\beta_1\beta_2\beta_3$ with integers $\beta_i$ of any sign satisfying (6.7). When $n$ is odd and square free, a direct computation shows that

$$\nu(n) = 2 \cdot 4^{\omega(n)}.$$

Therefore we conclude that

$$S^{\text{MT}}(x) = \sum_{1 \le n \le x} \mu^2(2n), \tag{6.8}$$

which corresponds to the first term on the right-hand side of (1.3).

## 7. Preparation of the error term: Part I

Let $S^{\text{Err}}(x)$ be the contribution to $S(x)$ of the terms $\boldsymbol{\beta}$ such that at least one $\beta_k$ (and hence at least two) is not an integer. Our goal is to prove that

$$S^{\text{Err}}(x) = O(x(\log x)^{-1/8}), \tag{7.1}$$

which combined with (6.8) will give (1.3) and hence Theorem 1.4.

### 7.1. Factorisation of the variables

We appeal to Lemma 4.1 to factorise each Gaussian integer $\beta_k$ in (6.5). The summation over the four variables $\beta_k$ is replaced by 20 variables $\eta_k$, $b_k$, $z_{k\ell}$. We take time to precisely write this expression, where we exchanged the indices 1 and 3 in comparison with (6.5). We have

$$S^{\text{Err}}(x) = \frac{1}{2} \sum_{\boldsymbol{\eta}} \sum_{\boldsymbol{b}} \frac{1}{4^{\omega(\Pi \boldsymbol{b})}} \sum_{\boldsymbol{z}} \frac{\mu^2\big(2(\Pi \boldsymbol{b})\,(\Pi \boldsymbol{z})\big)}{2^{\widetilde{\omega}(\Pi \boldsymbol{z})}} \Big[\frac{\eta_0 b_0 z_{01} z_{02} z_{03}}{\eta_1 b_1 z_{10} z_{12} z_{13}}\Big] \cdot \Big[\frac{\eta_2 b_2 z_{20} z_{21} z_{23}}{\eta_3 b_3 z_{30} z_{31} z_{32}}\Big], \tag{7.2}$$

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

where $\Pi \boldsymbol{b} := b_0 b_1 b_2 b_3$, $\Pi \boldsymbol{z} = \prod_{k \neq \ell} z_{k\ell} = \prod_{0 \leq k < \ell \leq 3} |z_{k\ell}|^2$ and

- we have
$$1 \leq (\Pi \boldsymbol{b})(\Pi \boldsymbol{z}) \leq x, \tag{7.3}$$
- $\boldsymbol{\eta} = (\eta_0, \eta_1, \eta_2, \eta_3)$ belongs to $\mathbb{U}^4$ and satisfies the equality
$$\eta_0 \eta_1 \eta_2 \eta_3 = 1, \tag{7.4}$$
- $\boldsymbol{b} = (b_0, b_1, b_1, b_3)$ is a four-tuple of odd positive integers,
- $\boldsymbol{z} = (z_{k\ell})_{0 \leq k \neq \ell \leq 3}$ are primitive primary Gaussian integers such that
$$z_{k\ell} = \overline{z_{\ell k}} \text{ for } 0 \leq k < \ell \leq 3, \tag{7.5}$$
- we have
$$\eta_0 \eta_3 b_0 b_3 z_{01} z_{02} z_{31} z_{32} |z_{03}|^2 \equiv \pm 1 \bmod 4, \ \eta_3 b_3 \text{ and } \eta_1 b_1 \text{ are primary, and} \tag{7.6}$$
- for some $0 \leq k \leq 3$, we have
$$\eta_k b_k \prod_{\ell \neq k} z_{k\ell} \notin \mathbb{Z}. \tag{7.7}$$

### 7.2. Comments and simplifications of (7.2)

Note that the factor $\mu^2(2(\Pi \boldsymbol{b})(\Pi \boldsymbol{z}))$ in the definition of $S^{\mathrm{Err}}(x)$ ensures that all the $b_k$ and all the $z_{k\ell}$ are odd and coprime by pairs. The integer $\Pi \boldsymbol{z}$ is only divisible by odd natural primes congruent to 1 mod 4, and and this remark leads to the equality

$$\widetilde{\omega}(\Pi \boldsymbol{z}) = 2\omega_1(\Pi \boldsymbol{z}) = 2\omega(\Pi \boldsymbol{z}). \tag{7.8}$$

Now consider the second part of (7.6). Since $b_1$ and $b_3$ are positive integers, the units $\eta_1$ and $\eta_3$ can only be equal to $\pm 1$. Hence the conditions $\eta_1 b_1$ and $\eta_3 b_3$ primary are equivalent to

$$b_1 \equiv \eta_1 \text{ and } b_3 \equiv \eta_3 \bmod 4. \tag{7.9}$$

Consider now the first part of (7.6). Since $|z_{03}|^2$ is a positive integer $\equiv 1 \bmod 4$, since $b_0$ and $b_3$ are $\equiv \pm 1 \bmod 4$, since $\eta_3 = \pm 1$ and since the $z_{k\ell}$ are primary, we deduce that $\eta_0 \equiv \pm 1 \bmod 2(1+i)$, so we have $\eta_0 = \pm 1$. Returning to (7.4), we deduce that $\eta_2 = \pm 1$. Thus we have

$$\boldsymbol{\eta} \in \{\pm 1\}^4, \text{ and } \eta_0 \eta_1 \eta_2 \eta_3 = 1. \tag{7.10}$$

With these remarks, we see that the first part of (7.6) is equivalent to

$$z_{01} z_{02} z_{31} z_{32} \equiv \pm 1 \bmod 4. \tag{7.11}$$

Since the value of every $\eta_k$ is $\pm 1$, we see that (7.7) is equivalent to

$$\text{for some } 0 \leq k < \ell \leq 3 \text{ we have } z_{k\ell} \neq 1. \tag{7.12}$$

That (7.7) implies (7.12) is clear. For the other direction, suppose, for instance, that $b_0 z_{01} z_{02} z_{03} = b'$, where $b'$ is some integer, and suppose that the primitive primary element

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

$z_{01}$ is not equal to 1. Then $z_{01}$ is divisible by some irreducible $\pi$, with $\pi\overline{\pi}$ an element of $\mathcal{P}^{\mathrm{odd}}$ congruent to 1 modulo 4. Necessarily, $\overline{\pi}$ divides the integer $b'$ and hence $\overline{\pi}$ divides $b_0$, $z_{02}$ or $z_{03}$. But $\overline{\pi}$ does not divide the integer $b_0$ (otherwise $b_0$ and $z_{01}$ would not be coprime). So $\overline{\pi}$ divides $z_{02}$, for instance. But by conjugation, $\overline{\pi}$ divides $\overline{z_{01}} = z_{10}$. So $z_{10}$ and $z_{02}$ would not be coprime, and this is a contradiction.

Finally, by the values of the symbol $[\frac{\cdot}{\cdot}]$ given in (4.2) and (4.4), we can suppress the $\eta_k = \pm 1$ in the numerators and denominators of both symbols $[\frac{\cdot}{\cdot}]$ in (7.2).

We benefit from all these remarks to simplify (7.2). So we introduce the set $\mathcal{U} \subset (\mathbb{Z}[i]/4\mathbb{Z}[i])^4$ defined by

$$\mathcal{U} := \big\{(u_{01}, u_{02}, u_{13}, u_{23}) : u_{01}\, u_{02}\, \overline{u_{13}}\, \overline{u_{23}} \equiv \pm 1 \bmod 4\big\}.$$

After a decomposition of (7.11) into congruences modulo 4 and a trivial summation over $\boldsymbol{\eta}$ and the $\boldsymbol{b}$ satisfying (7.9) and (7.10), we split $S^{\mathrm{Err}}(x)$ into

$$S^{\mathrm{Err}}(x) = \sum_{\boldsymbol{u}\in\mathcal{U}} S(x, \boldsymbol{u}),$$

with

$$S(x, \boldsymbol{u}) = \sum_{\boldsymbol{b}} \frac{1}{4^{\omega(\Pi b)}} \sum_{\boldsymbol{z}} \frac{\mu^2\big(2(\Pi \boldsymbol{b})\,(\Pi \boldsymbol{z})\big)}{2^{\widetilde{\omega}(\Pi z)}} \Big[\frac{b_0 z_{01} z_{02} z_{03}}{b_1 z_{10} z_{12} z_{13}}\Big] \cdot \Big[\frac{b_2 z_{20} z_{21} z_{23}}{b_3 z_{30} z_{31} z_{32}}\Big], \tag{7.13}$$

where $\boldsymbol{b}$ and $\boldsymbol{z}$ satisfy (7.5), (7.3), (7.12) and the congruence conditions

$$z_{01} \equiv u_{01}, z_{02} \equiv u_{02}, z_{13} \equiv u_{13}, z_{23} \equiv u_{23} \bmod 4. \tag{7.14}$$

The sum $S(x, \boldsymbol{u})$ contains 10 independent variables of summation:

$$b_0, b_1, b_2, b_3 \in \mathbb{N} \text{ and } z_{01}, z_{02}, z_{03}, z_{12}, z_{13}, z_{23} \in \mathbb{Z}[i], \tag{7.15}$$

since the other $z_{k\ell}$ are linked to each other by (7.5). The variables $b_k$ and $z_{k\ell}$ do not have the same role. Each variable $b_k$ appears in exactly one of the two symbols $[\frac{\cdot}{\cdot}]$, and thanks to (4.6) the variables $b_k$ play a similar role. The variable $z_{k\ell}$ and its conjugate $z_{\ell k} = \overline{z_{k\ell}}$ appear exactly once. But $z_{01}$ and $z_{10}$ appear in the numerator and the denominator of the same symbol. The same is true for $z_{23}$ and $z_{32}$. The other $z_{k\ell}$ and $z_{\ell k}$ appear in different symbols. In its combinatorial aspect, this situation appears to be different from the one encountered in [16], for instance.

### 7.3. Trivial bounds for some subsums of $S(x, u)$

We first give a trivial bound for the complete sum $S(x, \boldsymbol{u})$. Consider (7.13). Since every $p \equiv 1 \bmod 4$ can be written in 12 ways as

$$p = \prod_{0\le k\ne \ell\le 3} z_{k\ell},$$

where the primitive primary Gaussian integers $z_{k\ell}$ satisfy the conjugacy condition (7.5), we deduce the following trivial inequality for $S(x, \boldsymbol{u})$, where we bound each character by

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

1 and drop (7.14):

$$|S(x,\boldsymbol{u})| \leq \sum_{\boldsymbol{b}} \frac{1}{4^{\omega(\Pi \boldsymbol{b})}} \sum_{\substack{m \\ p|m \Rightarrow p \equiv 1 \bmod 4}} \mu^2(2(\Pi \boldsymbol{b})m) \cdot \frac{12^{\omega(m)}}{4^{\omega(m)}}. \tag{7.16}$$

Here we used (7.8), and the sum is over the positive integers $\boldsymbol{b} = (b_0, b_1, b_1, b_3)$ and $m$ such that $(\Pi \boldsymbol{b})m \leq x$. A direct application of Lemma 4.2 implies the bound

$$\begin{aligned} |S(x,\boldsymbol{u})| &\ll \sum_{b \leq x} \mu^2(2b) \frac{4^{\omega(b)}}{4^{\omega(b)}} (x/b) \mathcal{L}^{1/2} \\ &\ll x\mathcal{L}^{3/2}. \end{aligned}$$

As a consequence of (1.4), we see that this crude bound of the error term is larger than $S^{\mathrm{MT}}(x)$ by a small power of $\mathcal{L}$.

We want to generalise this bound to some important subsums we will meet in the sequel of the proof. Let $\mathcal{R}$ be a set of positive integers less than $x$. Let $S_{\mathcal{R}}(x,\boldsymbol{u})$ be the subsum of $S(x,\boldsymbol{u})$ corresponding to the further restriction on the variables

$$(\Pi \boldsymbol{b})(\Pi \boldsymbol{z}) \in \mathcal{R}.$$

We have the following lemma:

**Lemma 7.1.** *Uniformly for $x \geq 1$ and for $\mathcal{R}$ a subset of integers less than $x$, we have*

$$S_{\mathcal{R}}(x,\boldsymbol{u}) \ll (x|\mathcal{R}|)^{1/2}\mathcal{L}^{15/4}.$$

**Proof.** Let $g$ be the multiplicative function defined on the set of odd, square free integers by the formula

$$g(p) = \begin{cases} 4 & \text{if } p \equiv 1 \bmod 4, \\ 1 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

By a computation similar to (7.16) and by the Cauchy–Schwarz inequality, we have

$$\big|S_{\mathcal{R}}(x,\boldsymbol{u})\big| \leq \sum_{r \in \mathcal{R}} g(r) \leq \big|\mathcal{R}\big|^{1/2} \Big( \sum_{n \leq x} g^2(n) \Big)^{1/2}. \tag{7.17}$$

Let $h_1$ and $h_3$ be the two multiplicative functions defined on the set of square free integers by the formulas

$$h_1(p) = \begin{cases} 16 & \text{if } p \equiv 1 \bmod 4, \\ 0 & \text{if } p \equiv 3 \bmod 4, \end{cases} \quad \text{and } h_3(p) = \begin{cases} 0 & \text{if } p \equiv 1 \bmod 4, \\ 1 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

We have the convolution equality $g^2 = h_1 \star h_3$. It remains to apply Lemma 4.2 twice to obtain

$$\sum_{n \leq x} g^2(n) \ll x\mathcal{L}^{15/2}.$$

By (7.17) we complete the proof of Lemma 7.1. □

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

## 8. Preparation of the error term: Part II

### 8.1. Dissection of the domain of summation

We continue to prepare the error term $S(x, \boldsymbol{u})$ by controlling the sizes of the 10 variables appearing in (7.15) and removing the multiplicative constraint (7.3). When this is achieved, we will be in a good position to apply Lemmas 5.1, 5.2 and 5.4. Let $\Delta$ be the the dissection parameter

$$\Delta := (1+\mathcal{L}^{-10}).$$

We denote by $B_k$ and $Z_{k\ell}$ $(0 \le k \ne \ell \le 3)$ any number taken in the set of powers of $\Delta$

$$\{1, \Delta, \Delta^2, \Delta^3, \dots\},$$

and we impose $Z_{k\ell} = Z_{\ell k}$, for $k \ne \ell$ as a consequence of (7.5). We define

$$\boldsymbol{B} := (B_0, \dots, B_3), \boldsymbol{Z} := (Z_{k\ell}), \Pi\boldsymbol{B} := B_0B_1B_2B_3, \Pi\boldsymbol{Z} := |Z_{01}Z_{02}Z_{03}Z_{12}Z_{13}Z_{23}|^2.$$

The notation $b_k \simeq B_k$ (resp. $z_{k\ell} \simeq Z_{k\ell}$) means that the integer variable of summation $b_k$ (resp. the primitive primary Gaussian integer $z_{k\ell}$) satisfies the inequalities $B_k \le b_k < \Delta B_k$ (resp. $Z_{k\ell} \le |z_{k\ell}| < \Delta Z_{k\ell}$). More generally, the notation $\boldsymbol{b} \simeq \boldsymbol{B}$ means that for each $0 \le k \le 3$, we have $b_k \simeq B_k$. Then the notation $\boldsymbol{z} \simeq \boldsymbol{Z}$ has an obvious meaning. For $(\boldsymbol{B}, \boldsymbol{Z})$ as before, we consider the *cuboid*

$$\mathcal{C}(\boldsymbol{B}, \boldsymbol{Z}) := \prod_{0\le k\le 3} \Big[B_k, \Delta B_k\Big] \times \prod_{0\le k\ne\ell\le 3} \Big[Z_{k\ell}, \Delta Z_{k\ell}\Big]. \tag{8.1}$$

We return to (7.13). We cover the set of summation defined by (7.3) by

$$O(\mathcal{L}^{110}) \tag{8.2}$$

disjoint cuboids of the form $\mathcal{C}(\boldsymbol{B}, \boldsymbol{Z})$.

If $\mathcal{C}(\boldsymbol{B}, \boldsymbol{Z})$ is such that

$$(\Pi\boldsymbol{B})(\Pi\boldsymbol{Z})\Delta^{16} \le x,$$

then every element $(\boldsymbol{b}, \boldsymbol{z})$ of $\mathcal{C}(\boldsymbol{B}, \boldsymbol{Z})$ satisfies (7.3).

By contrast, if

$$(\Pi\boldsymbol{B})(\Pi\boldsymbol{Z}) \le x \text{ and } (\Pi\boldsymbol{B})(\Pi\boldsymbol{Z})\Delta^{16} > x,$$

the elements $(\boldsymbol{b}, \boldsymbol{z})$ of $\mathcal{C}(\boldsymbol{B}, \boldsymbol{Z})$ do not necessarily satisfy (7.3). However, the contribution of these elements to $S(x, \boldsymbol{u})$ is negligible. It suffices to apply Lemma 7.1, with

$$\mathcal{R} = [x(1 - O(\mathcal{L}^{-10}), x],$$

to see that the contribution is $\ll (x^2\mathcal{L}^{-10})^{1/2}\mathcal{L}^{15/4} \ll x\mathcal{L}^{-1/8}$, which fits in the error term of (7.1).

Similarly, the contribution to $S^{\mathrm{Err}}(x)$ of the union of the $\mathcal{C}(\boldsymbol{B}, \boldsymbol{Z})$ such that

$$(\Pi\boldsymbol{B})(\Pi\boldsymbol{Z}) \le x\mathcal{L}^{-10}$$

is also negligible. To prove that, we apply Lemma 7.1, with $\mathcal{R} = [1, x\mathcal{L}^{-10}]$, to see that this contribution is $\ll x\mathcal{L}^{-1/8}$.

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

### 8.2. The case of cuboids with too many small edges

Our purpose is to restrict our study to the cuboids $\mathcal{C}(\boldsymbol{B},\boldsymbol{Z})$ which have at least four *large* edges. So we introduce the following definition:

**Definition 8.1.** Let $\mathcal{C}(\boldsymbol{B},\boldsymbol{Z})$ be the cuboid defined in (8.1). Let $y$ be one of the 10 independent variables of the list in (7.15) and let $[Y,\Delta Y]$ be the edge associated to this variable $y$. We say that this edge is *large* if

(i) $Y \geq \exp(\mathcal{L}^{1/100})$ when $y$ is one of the $b_k$ $(0\leq k\leq 3)$ and

(ii) $Y \geq \mathcal{L}^{5000}$ when $y$ is one of the $z_{k\ell}$ $(0\leq k<\ell\leq 3)$.

If $Y$ does not satisfy these inequalities, we say that this edge is *small*.

Similarly, we say that the associated variable $y$ is large or small according to the inequality satisfied by $Y$.

Let $S_{\geq 7}(x,\boldsymbol{u})$ be the total contribution to $S(x,\boldsymbol{u})$ of all the $\mathcal{C}(\boldsymbol{B},\boldsymbol{Z})$ which have at least seven small edges associated to seven of the 10 independent variables of (7.15). We prove the following lemma:

**Lemma 8.2.** *For $x\geq 1$, we have*

$$S_{\geq 7}(x,\boldsymbol{u}) \ll x\mathcal{L}^{-1/8}.$$

**Proof.** The definition of *small* depends on the variable considered, and since the variables $b_k$ and $z_{k\ell}$ do not have the same role, we are obliged to consider different cases according to the respective number of $b_k$ and $z_{k\ell}$, which are large. However, we present only the case where at most two $b_k$ (say, $b_2$ and $b_3$) and at most one $z_{k\ell}$ (say, $z_{23}$) is large. The other cases are similar. Returning to (7.13), we see that the total contribution (denoted by $\Sigma(x)$) to $S(x,\boldsymbol{u})$ of the $\mathcal{C}(\boldsymbol{B},\boldsymbol{Z})$ corresponding to this particular case satisfies the inequality

$$|\Sigma(x)| \leq \sum_{b_0,\,b_1\leq \exp(\mathcal{L}^{1/100})}\sum \frac{1}{4^{\omega(b_0b_1b_2b_3)}} \sum_{\substack{|z_{01}|,|z_{02}|,|z_{03}|,\\ |z_{12}|,|z_{13}|\leq \mathcal{L}^{5000}}} \frac{1}{4^{\omega(|z_{01}\cdots z_{13}|^2)}} \sum_{b_2b_3\leq x/(b_0b_1|z_{01}|^2\cdots)}\sum \frac{1}{4^{\omega(b_2b_3)}} \sum_{|z_{23}|^2\leq x/(b_0b_1\cdots|z_{01}|^2\cdots)} \frac{1}{4^{\omega(|z_{23}|^2)}},$$

where all the prime factors of the integers $|z_{k\ell}|^2$ are congruent to 1 modulo 4. By the change of variables $b:=b_0b_1$, $m:=|z_{01}|^2|z_{02}|^2|z_{03}|^2|z_{12}|^2|z_{13}|^2$, $b'=b_2b_3$ and $m':=|z_{23}|^2$, we obtain the bound

$$|\Sigma(x)| \leq \sum_{b\leq \exp(2\mathcal{L}^{1/100})} \frac{1}{2^{\omega(b)}} \sum_{\substack{m\leq \mathcal{L}^{50000}\\ p\mid m\Rightarrow p\equiv 1 \bmod 4}} \Big(\frac{5}{2}\Big)^{\omega(m)} \sum_{b'\leq x/(bm)} \frac{1}{2^{\omega(b')}} \sum_{\substack{m'\leq x/(bb'm)\\ p\mid m'\Rightarrow p\equiv 1 \bmod 4}} \frac{1}{2^{\omega(m')}},$$

which is finally

$$\Sigma(x) \ll x\mathcal{L}^{-1/4+1/200+\varepsilon},$$

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

by a repeated application of Lemma 4.2 and where $\varepsilon > 0$ is arbitrary. This finally gives

$$\Sigma(x) \ll x\mathcal{L}^{-1/8},$$

as desired. □

### 8.3. The crucial sums

Let $(\boldsymbol{B}, \boldsymbol{Z})$ be as in §8.1 and let $S(\boldsymbol{B}, \boldsymbol{Z}, \boldsymbol{u})$ be the subsum of $S(x, \boldsymbol{u})$ (see (7.13)) defined by

$$S(\boldsymbol{B}, \boldsymbol{Z}, \boldsymbol{u}) = \sum_{\boldsymbol{b}} \frac{1}{4^{\omega(\Pi \boldsymbol{b})}} \sum_{\boldsymbol{z}} \frac{\mu^2\big(2(\Pi \boldsymbol{b})\,(\Pi \boldsymbol{z})\big)}{2^{\widetilde{\omega}(\Pi \boldsymbol{z})}} \Big[\frac{b_0 z_{01} z_{02} z_{03}}{b_1 z_{10} z_{12} z_{13}}\Big] \cdot \Big[\frac{b_2 z_{20} z_{21} z_{23}}{b_3 z_{30} z_{31} z_{32}}\Big], \tag{8.3}$$

where $\boldsymbol{b} = (b_k)_{0 \le k \le 3}$ and $\boldsymbol{z} = (z_{k\ell})_{0 \le k \ne \ell \le 3}$ satisfy (7.5), (7.12), (7.14) and

$$\boldsymbol{b} \simeq \boldsymbol{B} \text{ and } \boldsymbol{z} \simeq \boldsymbol{Z}.$$

Recall that $b_k$ are positive integers and $z_{k\ell}$ are primitive primary Gaussian integers.

By the discussion developed in §8.1, we can suppose that $(\boldsymbol{B}, \boldsymbol{Z})$ satisfies the inequalities

$$x\mathcal{L}^{-10} < (\Pi \boldsymbol{B})(\Pi \boldsymbol{Z}) \le x\Delta^{-16}. \tag{8.4}$$

By Lemma 8.2, we can restrict our study to the cuboids $\mathcal{C}(\boldsymbol{B}, \boldsymbol{Z})$ with

$$\text{at least four large variables among the 10 in (7.15).} \tag{8.5}$$

Finally, since the number of subsums $S(\boldsymbol{B}, \boldsymbol{Z}, \boldsymbol{u})$ is bounded by (8.2), to prove (7.1) it is sufficient to prove that for every $(\boldsymbol{B}, \boldsymbol{Z})$ satisfying (8.4) and (8.5) and for every $\boldsymbol{u} \in \mathcal{U}$, we have

$$S(\boldsymbol{B}, \boldsymbol{Z}, \boldsymbol{u}) \ll x\mathcal{L}^{-1/8-110}. \tag{8.6}$$

## 9. Proof of Theorem 1.4

The purpose of this section is to prove (8.6) by exploiting the oscillation of the character $[\cdot;\cdot]$ in different ways.

### 9.1. Gymnastics on the product of two characters

Recall that $z_{k\ell} = \overline{z_{\ell k}}$. The 10 independent variables given in (7.15) appear in (8.3). Let

$$F(\boldsymbol{b}, \boldsymbol{z}) := \Big[\frac{b_0 z_{01} z_{02} z_{03}}{b_1 z_{10} z_{12} z_{13}}\Big] \cdot \Big[\frac{b_2 z_{20} z_{21} z_{23}}{b_3 z_{30} z_{31} z_{32}}\Big]. \tag{9.1}$$

First of all we want to factorise $F$ in a suitable way to apply bounds coming from Lemmas 5.1, 5.2 and 5.4. We will exploit the multiplicativity of the characters (4.3) and the fact that all the elements $b_k$ and $z_{k\ell}$ have an odd real part to apply (4.6). Finally, we will use the conjugation formula (4.5). To shorten formulas, we introduce the following notation: let $x$ be one of 10 variables listed in (7.15); we denote by $f(\widehat{x})$ any function of the 10 variables of (7.15) but independent of $x$.

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

**Lemma 9.1.** *Let $(x, y)$ be a pair of distinct variables in (7.15) such that $(x, y)$ or $(y, x)$ belongs to the set $\mathcal{E}$ of 26 pairs of variables defined by*

$$\begin{aligned}\mathcal{E} := \{\ &(b_0, b_1), \quad (b_0, z_{01}), \quad (b_0, z_{12}), \quad (b_0, z_{13}), \quad (b_1, z_{01}), \quad (b_1, z_{02}),\\ &(b_1, z_{03}), \quad (b_2, b_3), \quad (b_2, z_{03}), \quad (b_2, z_{13}), \quad (b_2, z_{23}), \quad (b_3, z_{02}),\\ &(b_3, z_{12}), \quad (b_3, z_{23}), \quad (z_{01}, z_{02}), \quad (z_{01}, z_{03}), \quad (z_{01}, z_{12}), \quad (z_{01}, z_{13}),\\ &(z_{02}, z_{03}), \quad (z_{02}, z_{12}), \quad (z_{02}, z_{23}), \quad (z_{03}, z_{13}), \quad (z_{03}, z_{23}), \quad (z_{12}, z_{13}),\\ &(z_{12}, z_{23}), \quad (z_{13}, z_{23})\ \}.\end{aligned}$$

*Then at least one of the following two is true:*

(i) *There exist functions $\xi$ and $\zeta$ with modulus less than 1 such that for all the values of the variables $(\boldsymbol{b}, \boldsymbol{z})$, we have*

$$F(\boldsymbol{b}, \boldsymbol{z}) = \xi(\widehat{x})\zeta(\widehat{y})\Big[\frac{x}{y}\Big].$$

(ii) *There exist functions $\xi$ and $\zeta$ with modulus less than 1 such that for all the values of the variables $(\boldsymbol{b}, \boldsymbol{z})$, we have*

$$F(\boldsymbol{b}, \boldsymbol{z}) = \xi(\widehat{x})\zeta(\widehat{y})\Big[\frac{x}{\overline{y}}\Big].$$

**Proof.** We only give the proof when $(x, y) = (z_{01}, z_{12})$. With obvious meanings for $\alpha$, $\beta$, $\gamma$ and $\delta$, write

$$\Big[\frac{b_0 z_{01} z_{02} z_{03}}{b_1 z_{10} z_{12} z_{13}}\Big] \cdot \Big[\frac{b_2 z_{20} z_{21} z_{23}}{b_3 z_{30} z_{31} z_{32}}\Big] = \Big[\frac{\alpha z_{01}}{\beta \overline{z_{01}} z_{12}}\Big] \cdot \Big[\frac{\gamma \overline{z_{12}}}{\delta}\Big], \tag{9.2}$$

and decompose the first character as

$$\Big[\frac{\alpha z_{01}}{\beta \overline{z_{01}} z_{12}}\Big] = \Big[\frac{\alpha}{\beta \overline{z_{01}}}\Big] \cdot \Big[\frac{\alpha}{z_{12}}\Big] \cdot \Big[\frac{z_{01}}{\beta \overline{z_{01}}}\Big] \cdot \Big[\frac{z_{01}}{z_{12}}\Big].$$

Combining with (9.2), the definitions of $\xi(\widehat{z_{01}})$ and $\zeta(\widehat{z_{12}})$ are obvious. □

**Remark 5.** Actually in the application to follow, we will never use the pairs $(b_k, b_\ell)$ of the set $\mathcal{E}$, since there is no oscillation of the symbol $[\frac{b_k}{b_\ell}]$, because its value is always 1 (see (4.8)).

Finally, a pair $(z_{k\ell}, z_{k'\ell'})$, with $k < \ell$, $k' < \ell'$ and $(k, \ell) \neq (k', \ell')$, belongs to the set $\mathcal{E}$ of Lemma 9.1 if and only if the intersection of the set of indices $\{k, \ell\} \cap \{k', \ell'\}$ contains exactly one element. This property implies that in any set of three distinct variables $z_{k_i \ell_i}$, with $1 \leq i \leq 3$ and $0 \leq k_i < \ell_i \leq 3$, there exist at least two indices $i$ and $j$ such that $(z_{k_i \ell_i}, z_{k_j \ell_j})$ belongs to $\mathcal{E}$.

### 9.2. The final steps

Our proof of (8.6) is based on the number of large edges (at least four) of the cuboid $\mathcal{C}(\boldsymbol{B}, \boldsymbol{Z})$ and the distribution of this number between the $b_k$ and the $z_{k\ell}$. Recall that the $z_{k\ell}$ are primary, primitive, square free and coprime by pairs. Our discussion is divided into four cases which do not exclude each other.

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

**9.2.1. The variables $b_0$, $b_1$, $b_2$ and $b_3$ are large and no $z_{k\ell}$ is large.** By (7.12), there is a $z_{k\ell} \neq 1$. By symmetry, we can suppose that we have $z_{01} \neq 1$. By the multiplicative properties of the symbol $\left[\frac{\cdot}{\cdot}\right]$ and by (4.7), we factorise $F(\boldsymbol{b}, \boldsymbol{z})$ defined in (9.1) as

$$F(\boldsymbol{b}, \boldsymbol{z}) = f(\widehat{b_0})\Big[\frac{b_0}{z_{10}z_{12}z_{13}}\Big] = f(\widehat{b_0})\Big(\frac{b_0}{|z_{01}z_{12}z_{13}|^2}\Big),$$

where $f(\widehat{b_0})$ is a function independent of $b_0$ of modulus less than one. Since the variables $z_{01}(\neq 1)$, $\overline{z_{01}}$, $z_{12}$, $\overline{z_{12}}$, $z_{13}$ and $\overline{z_{13}}$ are small, primitive, primary and coprime in pairs, the denominator $|z_{01}z_{12}z_{13}|^2$ is a nonsquare odd integer, satisfying the inequalities

$$1 < |z_{10}z_{12}z_{13}|^2 \leq \mathcal{L}^{30000}. \tag{9.3}$$

We deduce the following inequality:

$$|S(\boldsymbol{B}, \boldsymbol{Z}, \boldsymbol{u})| \leq \sum_{b_1 \simeq B_1} \frac{1}{4^{\omega(b_1)}} \sum_{b_2 \simeq B_2} \frac{1}{4^{\omega(b_2)}} \sum_{b_3 \simeq B_3} \frac{1}{4^{\omega(b_3)}} \sum_{\boldsymbol{z} \simeq \boldsymbol{Z}} \frac{1}{4^{\omega(\Pi \boldsymbol{z})}} \Big| \sum_{b_0 \simeq B_0} \frac{\mu^2(b_0)}{4^{\omega(b_0)}} \Big(\frac{b_0}{|z_{10}z_{12}z_{13}|^2}\Big)\Big|,$$

where, furthermore, $b_0$ is coprime with $r := 2b_1b_2b_3|z_{02}z_{03}z_{23}|^2$. We apply Lemma 5.1 to the inner sum on $b_0$, with a very large $A$. Then we sum trivially over the other variables: by (8.4), (9.3) and the inequality $\log B_0 \geq \mathcal{L}^{1/100}$, we obtain (8.6).

**9.2.2. Three variables $b_k$ are large and some $z_{k'\ell'}$ is large.** We can suppose that the variables $b_0$, $b_1$ and $b_2$ are large. It easy to check that for any choice $0 \leq k' < \ell' \leq 3$, at least one of the pairs $(b_0, z_{k'\ell'})$, $(b_1, z_{k'\ell'})$ and $(b_2, z_{k'\ell'})$ appears in the set $\mathcal{E}$ given in Lemma 9.1. To facilitate the exposition, suppose that we are in the case where this pair is $(b_0, z_{01})$. Thanks to this lemma, we have

$$|S(\boldsymbol{B}, \boldsymbol{Z})| \leq \sum_{b_1, b_2, b_3} \sum \sum \sum_{\substack{z_{02}, z_{03}, z_{12} \\ z_{13}, z_{23}}} \cdots \sum \Big| \sum_{b_0 \simeq B_0} \sum_{z_{01} \simeq Z_{01}} \xi(\widehat{b_0})\zeta(\widehat{z_{01}})\Big[\frac{b_0}{z_{01}}\Big]\Big|. \tag{9.4}$$

Inspired by the equality

$$\Big[\frac{b_0}{z_{01}}\Big] = \Big(\frac{b_0}{|z_{01}|^2}\Big),$$

we put $m := |z_{01}|^2$. The number of ways of representing $m$ in this form is $O(d(m))$. Hence the last double sum in (9.4) is of the shape $\Omega(\boldsymbol{\xi}', \boldsymbol{\zeta}, \Delta B_0, \Delta^2 Z_{01}^2)$, with $|\xi'(m)| \leq d(m)$. We apply Lemma 5.3, with the choice $K = \mathcal{L}^{150}$. By hypothesis, $B_0$ and $Z_{01}^2$ are large, so both are greater than $\mathcal{L}^{10000}$. This lemma gives a nontrivial bound for the last double sum in (9.4) by a factor $\mathcal{L}^{-147}$. Summing trivially over the variables $z_{02}, z_{03}, z_{12}, z_{13}, z_{23}, b_1, b_2, b_3$ in (9.4), we complete the proof of (8.6).

**9.2.3. Two $b_k$ are large and two $z_{k'\ell'}$ are large.** By directly checking all the possibilities for the two variables $b_k$ and the two variables $z_{k'\ell'}$, we claim that there is

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

a pair $(b_{k_0}, z_{k_0'\ell_0'})$ of these large variables in the set $\mathcal{E}$. As soon as this pair $(b_{k_0}, z_{k_0'\ell_0'})$ is found, the proof is similar to §9.2.2.

**9.2.4. Three $z_{k\ell}$ are large.** By Remark 5, there exists a pair of these large variables $(z_{k\ell}, z_{k'\ell'})$ in the set $\mathcal{E}$ of Lemma 9.1. For simplicity of notation, suppose that this pair is $(z_{01}, z_{02})$. This allows us to rearrange $S(\boldsymbol{B}, \boldsymbol{Z}, \boldsymbol{u})$ as follows:

$$|S(\boldsymbol{B}, \boldsymbol{Z}, \boldsymbol{u})| \leq \sum_{b_0, b_1, b_2, b_3} \cdots \sum \sum_{z_{03}, z_{12}, z_{13}, z_{23}} \cdots \sum \Big| \sum_{z_{01} \simeq Z_{01}} \sum_{z_{02} \simeq Z_{02}} \xi(\widehat{z_{01}}) \zeta(\widehat{z_{02}}) \Big[ \frac{z_{01}}{z_{02}} \Big] \Big|,$$

for some coefficients $\boldsymbol{\xi}$ and $\boldsymbol{\zeta}$ less than one in modulus. The double inner sum over $z_{01}$ and $z_{02}$ is of the form $\Xi(\boldsymbol{\xi}, \boldsymbol{\zeta}, \Delta^2 Z_{01}^2, \Delta^2 Z_{02}^2)$, which is studied in Lemma 5.4. Since $Z_{01}$ and $Z_{02}$ are larger than $\mathcal{L}^{5000}$, this lemma gives a nontrivial bound for the last double sum by a factor $\mathcal{L}^{-10000/9}$. It remains to sum trivially over the $b_k$ and the four remaining $z_{k\ell}$ to obtain the bound (8.6) in this last case.

The proof of (8.6) has been accomplished in all the configurations of cuboids satisfying (8.4) and (8.5). The proof of Theorem 1.4 is now complete. □

## 10. Proof of Theorem 1.1

We split

$$\#\{0 < n < x : n \text{ odd and square free, } \mathrm{rk}_4 \mathrm{Cl}(K_n) \neq \omega_3(n) - 1\}$$

in the set of generic $n$ and its complement. The cardinality of the latter set is $O\big(x \log^{-1/4}\big)$, so it remains to bound

$$g(x) := \#\{0 < n < x : n \text{ odd, square free and generic, } \mathrm{rk}_4 \mathrm{Cl}(K_n) \neq \omega_3(n) - 1\}.$$

By Theorem 1.4, there exists an absolute $C_0$ such that for all $x \geq 2$, we have

$$\sum_{n \leq x} \mu^2(2n) \Big( \frac{f(n)}{2^{\omega_3(n)-1}} \Big) \leq \sum_{n \leq x} \mu^2(2n) + C_0\, x \log^{-1/8} x.$$

By positivity, we deduce

$$\sum_{\substack{n \leq x \\ n \text{ generic}}} \mu^2(2n) \Big( \frac{f(n)}{2^{\omega_3(n)-1}} \Big) \leq \sum_{n \leq x} \mu^2(2n) + C_0\, x \log^{-1/8} x.$$

By rearranging, we obtain

$$\begin{aligned} \sum_{\substack{n \leq x \\ n \text{ generic}}} \mu^2(2n) \Big( \frac{f(n)}{2^{\omega_3(n)-1}} - 1 \Big) &\leq \sum_{\substack{n \leq x \\ n \text{ not generic}}} \mu^2(2n) + C_0\, x \log^{-1/8} x, \\ &\leq 2 C_0\, x \log^{-1/8} x, \end{aligned} \tag{10.1}$$

for sufficiently large $x$. We appeal to Theorem 1.3 to conclude that

$$\frac{f(n)}{2^{\omega_3(n)-1}} - 1 \geq 0,$$

https://doi.org/10.1017/S1474748020000651 Published online by Cambridge University Press

and that it is equal to zero if and only if $\mathrm{rk}_4\mathrm{Cl}(K_n) = \omega_3(n) - 1$ and $\geq 1$ if $\mathrm{rk}_4\mathrm{Cl}(K_n) \geq \omega_3(n)$. These remarks imply that the left–hand side of (10.1) is larger than $g(x)$. This completes the proof of Theorem 1.1. □

**Acknowledgements** We thank Florent Jouve for some numerical computations. We are also very grateful to Mark Shusterman for useful discussions regarding the function-field version of this problem. We appreciate the valuable comments of the anonymous referee, which greatly improved the readability of the manuscript. Peter Koymans and Carlo Pagano wish to thank the Max Planck Institute for Mathematics in Bonn for its financial support, great work conditions and inspiring atmosphere.

## References

[1] A. Azizi, A. Zekhnini and M. Taous, On the 2–class field tower of $\mathbb{Q}\left(\sqrt{p_1p_2}, i\right)$ and the Galois group of its second Hilbert 2–class field, *Collect. Math.* **65**(1) (2014), 131–141.

[2] A. Azizi, A. Zekhnini and M. Taous, On the unramified quadratic and biquadratic extensions of the field $\mathbb{Q}\left(\sqrt{d}, i\right)$, *Int. J. Algebra* **6**(21–24) (2012), 1169–1173.

[3] A. Azizi, A. Zekhnini and M. Taous, Structure of $\mathsf{Gal}\left(k_2^{(2)}/k\right)$ for some fields $k = \mathbb{Q}\left(\sqrt{2p_1p_2}, i\right)$ with $\mathsf{Cl}_2(k) \cong (2,2,2)$, *Abh. Math. Semin. Univ. Hambg.* **84**(2) (2014), 203–231.

[4] A. Azizi, A. Zekhnini and M. Taous, Coclass of $\mathsf{Gal}\left(k_2^{(2)}/k\right)$ for some fields $k = \mathbb{Q}\left(\sqrt{p_1p_2q}, \sqrt{-1}\right)$ with 2–class groups of types $(2,2,2)$, *J. Algebra Appl.* **15**(2) (2016), 1650027.

[5] A. Azizi, A. Zekhnini and M. Taous, On the strongly ambiguous classes of some biquadratic number fields, *Math. Bohem.* **141**(3) (2016), 363–384.

[6] A. Azizi, A. Zekhnini and M. Taous, On the capitulation of the 2–ideal classes of the field $\mathbb{Q}\left(\sqrt{p_1p_2q}, i\right)$ of type $(2,2,2)$, *Bol. Soc. Parana. Mat. (3)* **38**(4) (2020), 127–135.

[7] A. Azizi, A. Zekhnini, M. Taous and D. C. Mayer, Principalization of 2–class groups of type $(2,2,2)$ of biquadratic fields $\mathbb{Q}\left(\sqrt{p_1p_2q}, \sqrt{-1}\right)$, *Int. J. Number Theory* **11**(4) (2015), 1177–1215.

[8] A. Bartel and H. W. Lenstra Jr., On class groups of random number fields. Proceedings of the London Mathematical Society, Preprint, 2018, https://arxiv.org/abs/1803.06903

[9] M. Bhargava, The density of discriminants of quartic rings and fields, *Ann. of Math. (2)* **162**(2) (2005), 1031–1063.

[10] M. Bhargava, A. Shankar and J. Tsimerman, On the Davenport–Heilbronn theorems and second order terms, *Invent. Math.* **193**(2) (2013), 439–499.

[11] M. Bhargava and I. Varma, On the mean number of 2-torsion elements in the class groups, narrow class groups, and ideal groups of cubic orders and fields, *Duke Math. J.* **164**(10) (2015), 1911–1933.

[12] H. Cohen and H. W. Lenstra Jr., *Heuristics on Class Groups of number fields*, Number Theory, Noordwijkerhout 1983, 33–62, Lecture Notes in Math., **1068** (Springer, Berlin, 1984).

[13] H. Cohen and J. Martinet, Class groups of number fields: numerical heuristics, *Math. Comp.* **48**(177) (1987), 123–137.

[14] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields: II, *Proc. A* **322**(1551) (1971), 405–420.
[15] G.L. Dirichlet, Recherches sur les formes quadratiques à coëfficients et à indéterminées complexes: première partie, *J. Reine Angew. Math.* **24** (1842), 291–371.
[16] É. Fouvry and J. Klüners, On the 4-rank of class groups of quadratic number fields, *Invent. Math.* **167**(3) (2007), 455–513.
[17] É. Fouvry and J. Klüners, On the negative Pell equation, *Ann. of Math. (2)* **172**(3) (2010), 2035–2104.
[18] É. Fouvry and J. Klüners, The parity of the period of the continued fraction of $\sqrt{d}$, *Proc. Lond. Math. Soc. (3)* **101**(2) (2010), 337–391.
[19] É. Fouvry and J. Klüners, Weighted distribution of the 4-rank of class groups and applications, *Int. Math. Res. Not.* 2011(16) (**2011**), 3618–3656.
[20] É. Fouvry and P. Koymans, On Dirichlet biquadratic fields, Preprint, 2020, https://arxiv.org/abs/2001.05350
[21] A. Fröhlich, *Central Extensions, Galois Groups and Ideal Class Groups of Number Fields*, Contemp. Math., **24** (American Mathematical Society, Providence, 1983).
[22] W. Ho, A. Shankar and I. Varma, Odd degree number fields with odd class number, *Duke Math. J.* **167**(5) (2018), 995–1047.
[23] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math., **84** (Springer-Verlag, New York, 1990).
[24] J. Klys, The distribution of $p$–torsion in degree $p$ cyclic fields. Algebra and Number Theory, Preprint. 2016, https://arxiv.org/abs/1610.00226
[25] P. Koymans and C. Pagano, On the distribution of $\mathsf{Cl}(K)[l^\infty]$ for degree $l$ cyclic fields, Preprint, 2018, https://arxiv.org/abs/1812.06884
[26] P. Koymans and C. Pagano, Higher genus theory, Preprint, 2019, https://arxiv.org/abs/1909.13871
[27] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*, Monogr. Math. (Springer-Verlag, Berlin, 2000).
[28] Y. Liu, M. M. Wood and D. Zureick-Brown, A predicted distribution for Galois groups of maximal unramified extensions, Preprint, 2019, https://arxiv.org/abs/1907.05002
[29] H.L. Montgomery and R.C. Vaughan, *Multiplicative Number Theory: I. Classical Theory*, Cambridge Stud. Adv. Math., **97** (Cambridge University Press, Cambridge, 2007).
[30] C. Pagano and E. Sofos, 4-ranks and the general model for statistics of ray class groups of imaginary quadratic number fields, Preprint, 2017, https://arxiv.org/abs/1710.07587
[31] A. Smith, $2^\infty$-Selmer groups, $2^\infty$-class groups, and Goldfeld's conjecture, Preprint, 2017, https://arxiv.org/abs/1702.02325
[32] T. Taniguchi and F. Thorne, Secondary terms in counting functions for cubic fields, *Duke Math. J.* **162**(13) (2013), 2451–2508.
[33] I. Varma, The mean number of 3-torsion elements in ray class groups of quadratic fields, forthcoming in *Israel J. Math.*
[34] W. Wang and M. M. Wood, Moments and interpretations of the Cohen-Lenstra-Martinet heuristics, Preprint, 2019, https://arxiv.org/abs/1907.11201