Journal of Number Theory 200 (2019) 407–426

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the asymptotics of a prime spin relation

Christine McMeekin

ARTICLE INFO

Article history:
Received 2 July 2018
Received in revised form 5 November 2018
Accepted 10 November 2018
Available online 31 January 2019
Communicated by F. Pellarin

Keywords:
Density
Spin
Number theory
Asymptotic
Prime
Primes
Class field theory
Prime spin
Spin relation
Spin of prime ideals
Spin of a prime ideal

ABSTRACT

For certain cyclic totally real number fields, we give formulas for the density of primes that satisfy a given spin relation.

Contents

1. Introduction . . . 408
2. The spin of prime ideals . . . 410
3. Some class field theory . . . 411
4. An equidistribution lemma . . . 416
5. Property star and the starlight invariant . . . 418
6. Density theorems . . . 420

Acknowledgments . . . 425

References . . . 425

E-mail addresses: cem255@cornell.edu, christine.mcmeekin@gmail.com.

https://doi.org/10.1016/j.jnt.2018.11.027

1. Introduction

Let $K = K(n,\ell)$ denote a totally real number field that is cyclic over $\mathbb{Q}$ with odd prime degree n such that the class number of K is odd, 2 is inert, and every totally positive unit is a square. Let ℓ denote the conductor of K and let $\mathcal{O}_K$ denote the ring of integers of K.

Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma \neq 1$. Given an odd principal ideal $\mathfrak{a}$, following [FIMR13], we define the *spin* of $\mathfrak{a}$ (with respect to σ) to be

$$\mathrm{spin}(\mathfrak{a},\sigma) = \left(\frac{\alpha}{\mathfrak{a}^{\sigma}}\right)$$

where $\mathfrak{a} = (\alpha)$, α is totally positive, and $\left(\frac{\cdot}{\cdot}\right)$ denotes the quadratic residue symbol in K.

The main results of this paper give a formula for the density of rational primes that exhibit the spin relation

$$\mathrm{spin}(\mathfrak{p},\sigma) = \mathrm{spin}(\mathfrak{p},\sigma^{-1}) \quad \text{for all } \sigma \neq 1 \in \mathrm{Gal}(K/\mathbb{Q})$$

where $\mathfrak{p}$ is a prime of K above p. The formula is given in terms of $n = [K:\mathbb{Q}]$ and m_K, a computable and bounded invariant of the number field K. Define

$$\mathbf{M}_4 := (\mathcal{O}_K/4\mathcal{O}_K)^{\times}/\left((\mathcal{O}_K/4\mathcal{O}_K)^{\times}\right)^2$$

where $\mathcal{O}_K$ denotes the ring of integers of K. We define *the Starlight invariant* of the number field K (denoted m_K) to be the number of non-trivial $\mathrm{Gal}(K/\mathbb{Q})$-orbits of $\mathbf{M}_4$ with representative $\alpha \in \mathcal{O}_K$ such that the Hilbert symbol $(\alpha,\alpha^{\sigma})_2 = 1$ for all non-trivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

The main results of this paper are motivated by the following conjecture, which gives a computable and bounded formula for the density of rational primes with constant spin equal to 1.

Conjecture 1.1. *Fix $K := K(n,\ell)$. The density of rational primes p such that $\mathrm{spin}(\mathfrak{p},\sigma) = 1$ for all non-trivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is given by*

$$C_K := \frac{2^{n-1}(n-1) + m_K n + 1}{\left(\sqrt{2}\right)^{3n-1} n}.$$

Restricting to rational primes that split completely in $K/\mathbb{Q}$, the corresponding conditional density is given by

$$C_{K,S} := \frac{m_K n + 1}{\left(\sqrt{2}\right)^{3n-1}}.$$

The reasoning behind Conjecture 1.1 is as follows. We break up the density C_K into a product of two densities as though one might break up a probability into a product of conditional probabilities. Then C_K is the product of two densities; the first is D_K, the density of rational primes satisfying the spin relation given in Theorem 1.2, and the second is the conditional density of rational primes p with $\mathrm{spin}(\mathfrak{p}, \sigma) = 1$ for all non-trivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, assuming that p satisfies the spin relation. Conjecture 1.1 then asserts that

$$C_K = D_K \left(\frac{1}{2}\right)^{\left(\frac{n-1}{2}\right)}.$$

Note that the condition that p satisfies the spin relation is a Cebotarev condition so by Theorems 1.1 and 1.2 in [FIMR13], if $\mathrm{spin}(\mathfrak{p}, \sigma)$ and $\mathrm{spin}(\mathfrak{p}, \tau)$ are independent for $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$ with $\sigma \neq \tau, \tau^{-1}$, then we arrive at Conjecture 1.1.

A corollary of Conjecture 1.1 is a family of number fields $\{F_K(p)\}_p$ depending on p such that p is always ramified in $F_K(p)/\mathbb{Q}$ and the density of rational primes that split as completely as possible in $F_K(p)/\mathbb{Q}$ (given the ramification) is

$$\frac{C_{K,S}}{n}.$$

Theorem 1.2. *Let $K := K(n, \ell)$. The density of rational primes p that satisfy the spin relation*

$$\mathrm{spin}(\mathfrak{p}, \sigma) = \mathrm{spin}(\mathfrak{p}, \sigma^{-1}) \quad \textit{for all } \sigma \neq 1 \in \mathrm{Gal}(K/\mathbb{Q})$$

where $\mathfrak{p}$ is a prime of K above p is given by

$$D_K = \frac{2^{n-1}(n-1) + m_K n + 1}{2^n n}.$$

Theorem 1.3. *Let $K := K(n, \ell)$. Then*

$$0 < \frac{2^{n-1}(n-1) + 1}{2^n n} \leq D_K \leq \frac{1}{2}.$$

Table 1 gives examples of computed Starlight invariants for cyclic number fields of degree n over $\mathbb{Q}$ and conductor ℓ for the given n and ℓ values and it gives the corresponding density of primes satisfying the spin relation. These values of m_K were computed using magma [BCP97]; the code can be found in Appendix B of [McM18].

We remark that we can simplify the restrictions on K in the cubic case. For $n = 3$, the assumption that the class number of K is odd is sufficient to imply that every totally positive unit is a square due to results of Armitage and Fröhlich [AF67].

Table 1
Computed Starlight invariants and densities of the prime spin relation using Theorem 1.2.

n	3	5	7	11	13	17	19
ℓ	7	11	43	23	53	103	191
m_K	1	1	3	3	5	17	27
D_K	$\frac{1}{2}$	$\frac{7}{16}$	$\frac{29}{64}$	$\frac{467}{1024}$	$\frac{1893}{4096}$	$\frac{30849}{65536}$	$\frac{124187}{262144}$

Theorem 1.4 *([AF67]). Let K be a cyclic cubic number field with odd class number. Then every totally positive unit is a square.*

Proof. Let $U := \mathcal{O}_K^\times$ denote the group of units, U_T the totally positive units, and U^2 the square units. Observe $U^2 \subseteq U_T \subseteq U$. Then we have a surjective homomorphism

$$\phi : \frac{U}{U^2} \to \frac{U}{U_T}.$$

If none of the nontrivial class representatives of U/U^2 are totally positive then ϕ is injective. By Theorem V in [AF67], all signatures are represented by units. Square units are always totally positive and there are 8 signatures and 8 classes of units mod squares, so each class of U/U^2 must have a different signature. Therefore $U_T = U^2$. $\square$

2. The spin of prime ideals

Let $K := K(n, \ell)$ and let $h(K)$ denote the class number of K.

Definition 2.1 *([FIMR13]).* Let $\sigma \neq 1 \in \mathrm{Gal}(K/\mathbb{Q})$. Given an odd principal ideal $\mathfrak{a}$, we define the *spin* of $\mathfrak{a}$ (with respect to σ) to be

$$\mathrm{spin}(\mathfrak{a}, \sigma) = \left(\frac{\alpha}{\mathfrak{a}^\sigma}\right)$$

where $\mathfrak{a}^{h(K)} = (\alpha)$, α is totally positive, and $\left(\frac{\cdot}{\cdot}\right)$ denotes the quadratic residue symbol in K.

Spin is well-defined; since every totally positive unit is a square, the choice of totally positive generator α does not affect the quadratic residue and Lemma 3.1 asserts the existence of a totally positive generator.

Lemma 11.1 in [FIMR13] states that the product $\mathrm{spin}(\mathfrak{p}, \sigma)\mathrm{spin}(\mathfrak{p}, \sigma^{-1})$ is a product of Hilbert symbols at places dividing 2. We restate this more explicitly in Lemma 2.2.

For a place v of K, let $K_{(v)}$ denote the completion of K at v. For $a, b \in K$ co-prime to v, the Hilbert Symbol is defined such that $(a, b)_v := 1$ if the equation $ax^2 + by^2 = z^2$ has a solution $x, y, z \in K_{(v)}$ where at least one of x, y, or z is nonzero and $(a, b)_v := -1$ otherwise.

Lemma 2.2 *([FIMR13]). Let $K := K(n, \ell)$. Let α be a totally positive generator of the odd prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$. Then*

$$spin(\mathfrak{p}, \sigma) spin(\mathfrak{p}, \sigma^{-1}) = \prod_{v|2} (\alpha, \alpha^\sigma)_v.$$

In particular, if $\alpha \equiv 1 \bmod 4$ then $\prod_{v|2}(\alpha, \alpha^\sigma)_v = 1$. Since 2 is inert in $K/\mathbb{Q}$,

$$spin(\mathfrak{p}, \sigma) spin(\mathfrak{p}, \sigma^{-1}) = (\alpha, \alpha^\sigma)_2.$$

Proof. See Lemma 11.1 in [FIMR13] or use the standard fact of Hilbert symbols that $\prod_v (\alpha, \alpha^\sigma)_v = 1$. $\square$

3. Some class field theory

We now diverge momentarily from the spin of prime ideals to discuss some class field theory in the case when every totally positive unit is a square. We say a modulus is *narrow* whenever it is divisible by all infinite places. We say a modulus is *wide* whenever it is not divisible by any infinite place. We say a ray class group or ray class field is narrow or wide whenever its defining modulus is narrow or wide respectively. Let $U := \mathcal{O}_K^\times$ denote the group of units of K, let U_T denote the totally positive units, and let U^2 denote the square units. The following lemma is an exercise in class field theory.

Lemma 3.1. *Let K be a totally real number field. The following are equivalent.*

(1) *$U_T = U^2$.*
(2) *The narrow and wide Hilbert class groups of K coincide.*
(3) *Every principal ideal of K has a totally positive generator.*

Proof. To show the equivalence of (1) and (2), apply Theorem V.1.7 in [Mil13] using the modulus given by the product of all infinite places. Statements (3) and (2) are equivalent by the definitions of narrow and wide class groups. $\square$

Definition 3.2. Let $K := K(n, \ell)$. For q a power of 2, we define the group

$$\mathbf{M}_q := (\mathcal{O}_K / q\mathcal{O}_K)^\times \big/ \left((\mathcal{O}_K / q\mathcal{O}_K)^\times \right)^2.$$

The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts on $\mathbf{M}_q$ in the natural way.

We will primarily be interested in $\mathbf{M}_4$. We will see in Lemma 3.5 that $\mathbf{M}_q$ is canonically isomorphic to a quotient of the narrow ray class group over K of conductor q modulo squares.

Lemma 3.3 *([Mun]). Let K be a cyclic number field of odd degree n over $\mathbb{Q}$ such that 2 is inert in K. Then as vector spaces*

$$\mathbf{M}_4 \cong (\mathbb{Z}/2)^n.$$

Furthermore, the invariants of the action of $\mathrm{Gal}(K/\mathbb{Q})$ *are exactly* $\pm 1 \in \mathbf{M}_4$.

Proof. This proof is due to Sam Mundy [Mun]. Consider the exact sequence

$$0 \to 1 + 2(\mathcal{O}_K/4) \to (\mathcal{O}_K/4)^\times \to (\mathcal{O}_K/2)^\times \to 1. \tag{1}$$

Note that $\mathcal{O}_K/2 \cong \mathbb{F}_{2^n}$ because K is cyclic of odd degree and 2 is inert in K. Also, $G \cong \mathrm{Gal}(\mathbb{F}_{2^n}/\mathbb{F}_2)$.

Viewing $\mathbb{F}_{2^n}$ as an additive group with Galois action by $G \cong \mathrm{Gal}(\mathbb{F}_{2^n}/\mathbb{F}_2)$, there is an isomorphism of Galois modules given by

$$\psi : \mathbb{F}_{2^n} \cong \mathcal{O}_K/2 \to 1 + 2(\mathcal{O}_K/4)$$

$$\psi : x \mapsto 1 + 2x.$$

This map is easily seen to be a Galois equivariant homomorphism. Injectivity and surjectivity follow from considering 2-adic expansions of elements in $\mathcal{O}_K/4$. Since ψ is an isomorphism we can rewrite the exact sequence of Galois modules in equation 1 as

$$0 \to \mathbb{F}_{2^n} \to (\mathcal{O}_K/4)^\times \to \mathbb{F}_{2^n}^\times \to 1. \tag{2}$$

Next consider the diagram of exact sequences below.

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{F}_{2^n} \arrow[r] \arrow[d, "2(\cdot)"] & (\mathcal{O}_K/4)^\times \arrow[r] \arrow[d, "(\cdot)^2"] & \mathbb{F}_{2^n}^\times \arrow[r] \arrow[d, "(\cdot)^2"] & 1 \\
0 \arrow[r] & \mathbb{F}_{2^n} \arrow[r] & (\mathcal{O}_K/4)^\times \arrow[r] & \mathbb{F}_{2^n}^\times \arrow[r] & 1
\end{tikzcd}$$

The first vertical map is multiplication by 2, which is the zero map. The next two vertical maps are squaring. The third vertical map is an isomorphism because $\mathbb{F}_{2^n}^\times$ is cyclic of odd order. Recall that

$$\mathbf{M}_4 := (\mathcal{O}_K/4\mathcal{O}_K)^\times\ /\text{squares}.$$

Then we apply the snake lemma to the diagram below.

$$\begin{tikzcd}
 & & & 1 \arrow[d] & \\
0 \arrow[r] & \mathbb{F}_{2^n} \arrow[r] \arrow[d, "0"] & (\mathcal{O}_K/4)^\times \arrow[r] \arrow[d, "(\cdot)^2"] & \mathbb{F}_{2^n}^\times \arrow[r] \arrow[d, "(\cdot)^2"] & 1 \\
0 \arrow[r] & \mathbb{F}_{2^n} \arrow[r] \arrow[d] & (\mathcal{O}_K/4)^\times \arrow[r] \arrow[d] & \mathbb{F}_{2^n}^\times \arrow[r] \arrow[d] & 1 \\
 & \mathbb{F}_{2^n} \arrow[r] & \mathbf{M}_4 \arrow[r] & 1 &
\end{tikzcd}$$

The snake lemma gives us the exact sequence of G-modules

$$0 \to \mathbb{F}_{2^n} \to \mathbf{M}_4 \to 1.$$

Therefore $\mathbf{M}_4 \cong \mathbb{F}_{2^n}$ as G-modules. The invariants of $\mathbb{F}_{2^n}$ are $\mathbb{F}_2$. Tracing through the isomorphism we see that this corresponds to the invariants $\{\pm 1\}$ in $\mathbf{M}_4$. $\square$

Let $\mathbb{M}_{q,G}$ denote the set of $\mathrm{Gal}(K/\mathbb{Q})$-orbits of $\mathbf{M}_q$ for q a power of 2. Recall that we say a modulus of K is narrow whenever $\mathfrak{m}_\infty$ divides the modulus where $\mathfrak{m}_\infty$ is the product of all infinite places of K. Letting $\mathfrak{m}$ denote a narrow modulus with finite part $\mathfrak{m}_0$, let $J_K^{\mathfrak{m}} = J_K^{\mathfrak{m}_0}$ denote the group of fractional ideals of K prime to $\mathfrak{m}_0$ and let $P_K^{\mathfrak{m}} = P_K^{\mathfrak{m}_0}$ denote the subgroup of $J_K^{\mathfrak{m}}$ formed by the principal ideals with generator $\alpha \in K^\times$ such that $\mathrm{ord}_2(q) \le \mathrm{ord}_2(\alpha)$ and $\alpha \succ 0$. We let $\mathscr{P}_K^{\mathfrak{m}} = \mathscr{P}_K^{\mathfrak{m}_0}$ denote the set of prime ideals of $\mathcal{O}_K$ co-prime to $\mathfrak{m}_0$ so that $J_K^{\mathfrak{m}}$ is generated by $\mathscr{P}_K^{\mathfrak{m}}$.

Definition 3.4. Let $K := K(n, \ell)$. Let $q \ge 4$ be a power of 2.

(1) Define the map

$$\begin{aligned} \mathbf{r}_0 : \mathscr{P}_K^2 &\to \mathbf{M}_q \\ \mathfrak{p} &\mapsto \alpha \end{aligned}$$

where $\alpha \in \mathcal{O}_K$ is a totally positive generator for the principal ideal $\mathfrak{p}^{h(K)}$.

(2) Define the map

$$\begin{aligned} \mathbf{r} : \mathscr{P}_{\mathbb{Q}}^2 &\to \mathbb{M}_{q,G} \\ p &\mapsto [\mathbf{r}_0(\mathfrak{p})] \end{aligned}$$

where $\mathfrak{p}$ is any prime in K above p. Here $[\alpha]$ denotes the $\mathrm{Gal}(K/\mathbb{Q})$-orbit of $\alpha \in \mathbf{M}_4$ considered in $\mathbb{M}_{q,G}$.

The map $\mathbf{r}_0$ is well-defined out of $\mathscr{P}_K^2$; recall that by Lemma 3.1, $U_T = U^2$ is equivalent to the coincidence of the narrow and wide Hilbert class groups so $U_T = U^2$ if and only if all principal ideals have a totally positive generator. Since squares are trivial in $\mathbf{M}_q$ by definition and $U_T = U^2$, the map $\mathbf{r}_0$ is well-defined.

The map $\mathbf{r}$ is well-defined out of $\mathscr{P}_{\mathbb{Q}}^2$ because $\mathbb{M}_{q,G}$ is the quotient of $\mathbf{M}_q$ by the $\mathrm{Gal}(K/\mathbb{Q})$-action so different choices of primes $\mathfrak{p}$ of K above p give the same result; $\mathbf{r}_0(\mathfrak{p}^\sigma) = \mathbf{r}_0(\mathfrak{p})^\sigma$ for $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and $\mathfrak{p}$ an odd prime of K.

Since J_K^q is generated by $\mathscr{P}_K^q = \mathscr{P}_K^2$, the map $\mathbf{r}_0$ induces a homomorphism

$$\varphi_0 : J_K^q \to \mathbf{M}_q.$$

Lemma 3.5. *Let $K := K(n, \ell)$. The homomorphism $\varphi_0 : J_K^q \to \mathbf{M}_q$ induces a canonical surjective homomorphism*

$$\varphi : \mathrm{n}\mathcal{C}\mathrm{l}_K^q \to \mathbf{M}_q.$$

Proof. We first show the induced homomorphism is well-defined. By Proposition V.1.6 in [Mil13], every element of $\mathrm{n}\mathcal{C}\mathrm{l}^q$ is represented by an integral ideal. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two integral ideals representing the same element of $\mathrm{n}\mathcal{C}\mathrm{l}^q$. Then by Proposition V.1.6 in [Mil13], there exist nonzero $a, b \in \mathcal{O}_K$ such that

$$\begin{aligned} &b\mathfrak{a} = a\mathfrak{b}, \\ &a \equiv b \equiv 1 \bmod q, \quad \text{and} \\ &ab \succ 0. \end{aligned}$$

Since $\varphi_0 : J_K^q \to \mathbf{M}_q$ is a homomorphism,

$$\varphi_0(b\mathcal{O}_K)\varphi_0(\mathfrak{a}) = \varphi_0(a\mathcal{O}_K)\varphi_0(\mathfrak{b}).$$

Noting that $h(K)$ is odd and squares are trivial in $\mathbf{M}_q$ by definition, φ_0 maps any principal integral ideal (α) to the class in $\mathbf{M}_q$ containing the representative $\alpha \in \mathcal{O}_K$ where α is a totally positive generator.

Since $U_T = U^2$, every principal ideal of $\mathcal{O}_K$ has a totally positive generator so there exists a unit $u \in \mathcal{O}_K^\times$ such that $ua \succ 0$ and $\varphi_0(a) = ua$. Since $ab \succ 0$, then $u^{-1}b \succ 0$ so $\varphi_0(b) = u^{-1}b$. We know that $a \equiv b \equiv 1 \bmod q$. Since squares are trivial in $\mathbf{M}_q$ by the definition of $\mathbf{M}_q$, this implies

$$\begin{aligned} &u^2 a \equiv b \quad \text{in } \mathbf{M}_q \\ \Longrightarrow\ &ua \equiv u^{-1}b \quad \text{in } \mathbf{M}_q \\ \Longrightarrow\ &\varphi_0(a\mathcal{O}_K) = \varphi_0(b\mathcal{O}_K) \\ \Longrightarrow\ &\varphi_0(\mathfrak{a}) = \varphi_0(\mathfrak{b}). \end{aligned}$$

Therefore the homomorphism φ_0 induces a well-defined homomorphism from $\mathrm{n}\mathcal{C}\mathrm{l}_K^q$.

We now show the homomorphism is a canonical surjective homomorphism. Let $\mathfrak{m}$ be the narrow modulus with finite part q. Let

$$\begin{aligned} K_{\mathfrak{m}} &:= \{a \in K^\times : \mathrm{ord}_2(a) = 0\}, \\ K_{\mathfrak{m},1} &:= \{a \in K^\times : \mathrm{ord}_2(a-1) \geq \mathrm{ord}_2(q), a \succ 0\}, \\ U_{\mathfrak{m},1} &:= K_{\mathfrak{m},1} \cap U. \end{aligned}$$

Let $X \in \mathbf{M}_q$. Consider the exact sequence from Theorem V.1.7 in [Mil13];

$$1 \to U/U_{\mathfrak{m},1} \to K_{\mathfrak{m}}/K_{\mathfrak{m},1} \to \mathrm{n}\mathcal{C}\mathrm{l}_K^{\mathfrak{m}} \to C \to 1$$

and the canonical isomorphism

$$K_{\mathfrak{m}}/K_{\mathfrak{m},1} \cong (\pm)^n \times (\mathcal{O}_K/q)^\times . \tag{3}$$

Consider only the 2-part of each group. Then since $h(K)$ is odd, we have the short exact sequence

$$1 \to (U/U_{\mathfrak{m},1})[2^\infty] \to (K_{\mathfrak{m}}/K_{\mathfrak{m},1})[2^\infty] \to (\mathrm{n}\mathcal{C}\mathrm{l}_K^{\mathfrak{m}})[2^\infty] \to 1.$$

Note that since squaring sends all signatures to the trivial signature, the canonical isomorphism in equation 3 induces a canonical isomorphism on the 2-part modulo squares;

$$(K_{\mathfrak{m}}/K_{\mathfrak{m},1})[2^\infty]/(K_{\mathfrak{m}}/K_{\mathfrak{m},1})[2^\infty]^2 \cong (\pm)^n \times \mathbf{M}_q.$$

Consider the squaring map and apply the snake lemma to get the following commutative diagram of exact sequences;

$$\begin{tikzcd}
1 \arrow[r] & (U/U_{\mathfrak{m},1})[2^\infty] \arrow[r] \arrow[d, "(\cdot)^2"] & (K_{\mathfrak{m}}/K_{\mathfrak{m},1})[2^\infty] \arrow[r] \arrow[d, "(\cdot)^2"] & (\mathrm{n}\mathcal{C}\mathrm{l}_K^q)[2^\infty] \arrow[r] \arrow[d, "(\cdot)^2"] & 1 \\
1 \arrow[r] & (U/U_{\mathfrak{m},1})[2^\infty] \arrow[r] \arrow[d] & (K_{\mathfrak{m}}/K_{\mathfrak{m},1})[2^\infty] \arrow[r] \arrow[d] & (\mathrm{n}\mathcal{C}\mathrm{l}_K^q)[2^\infty] \arrow[r] \arrow[d] & 1 \\
& U/U^2 \arrow[r] \arrow[d] & (\pm)^n \times \mathbf{M}_q \arrow[r, "\psi"] \arrow[d] & \mathrm{n}\mathcal{C}\mathrm{l}_K^q/(\mathrm{n}\mathcal{C}\mathrm{l}_K^q)^2 \arrow[r] \arrow[d] & 1 \\
& 1 & 1 & 1 &
\end{tikzcd}$$

Then ψ induces an isomorphism

$$\psi : ((\pm)^n \times \mathbf{M}_q)/\mathrm{image}(U/U^2) \longrightarrow \mathrm{n}\mathcal{C}\mathrm{l}_K^q/(\mathrm{n}\mathcal{C}\mathrm{l}_K^q)^2.$$

Tracing through the definitions of the maps, $\varphi \circ \psi$ is surjective (it is essentially the identity). Therefore φ is surjective. □

4. An equidistribution lemma

Definition 4.1. Let S be a set of primes and let $R \subseteq S$. If the limit exists, then the *restricted density* of R (restricted to S) is defined as

$$d(R|S) := \lim_{N\to\infty} \frac{\#R_N}{\#S_N}$$

where S_N and R_N denote the set of primes in S and R respectively of absolute norm less than $N \in \mathbb{Z}_+$.

Recall that $\mathscr{P}_{\mathbb{Q}}^{m}$ denotes the set of rational primes not dividing m and $\mathscr{P}_{K}^{\mathfrak{m}}$ denotes the set of primes of K not dividing $\mathfrak{m}$. Letting $\mathfrak{p}$ be a prime of K above a rational prime p, denote the corresponding inertia degree $f_{K/\mathbb{Q}}(p) = f_{K/\mathbb{Q}}(\mathfrak{p})$ (well-defined because K is Galois over $\mathbb{Q}$). That is,

$$f_{K/\mathbb{Q}}(p) = f_{K/\mathbb{Q}}(\mathfrak{p}) = \frac{\#D}{\#E}$$

where D is the decomposition group of $\mathfrak{p}$ for the extension $K/\mathbb{Q}$ and E is the inertia group.

Definition 4.2. Let $K = K(n, \ell)$. Define the following sets of rational primes.

$$S := \{p \in \mathscr{P}_{\mathbb{Q}}^{2\ell} : f_{K/\mathbb{Q}}(p) = 1\} \quad \text{and} \quad I := \{p \in \mathscr{P}_{\mathbb{Q}}^{2\ell} : f_{K/\mathbb{Q}}(p) = n\}.$$

Define the following sets of primes of K.

$$S' := \{\mathfrak{p} \in \mathscr{P}_{K}^{2\ell} : f_{K/\mathbb{Q}}(\mathfrak{p}) = 1\} \quad \text{and} \quad I' := \{\mathfrak{p} \in \mathscr{P}_{K}^{2\ell} : f_{K/\mathbb{Q}}(\mathfrak{p}) = n\}.$$

That is, $S \subseteq \mathscr{P}_{\mathbb{Q}}^{2\ell}$ is the set of odd rational primes that split completely in $K/\mathbb{Q}$ and $I \subseteq \mathscr{P}_{\mathbb{Q}}^{2\ell}$ is the set of odd rational primes that are inert in $K/\mathbb{Q}$. Furthermore, S' is the set of primes of K laying above the primes in S and I' is the set of primes of K laying above the primes in I.

Since $K/\mathbb{Q}$ is cyclic of prime degree n, then $f_{K/\mathbb{Q}}(p) = 1$ or n for all $p \in \mathscr{P}_{\mathbb{Q}}^{2\ell}$ so in this case, $\mathscr{P}_{\mathbb{Q}}^{2\ell}$ is the disjoint union of S and I. The next Lemma asserts that for $K := K(n, \ell)$, the primes are equidistributed in $\mathbf{M}_4$ via the map $\mathbf{r}_0$.

Although the equidistribution generalizes to $\mathbf{M}_q$, note that the number of elements of $\mathbf{M}_8$ for example is different than the number of elements of $\mathbf{M}_4$ so the generalized statement would need to be adjusted accordingly.

Lemma 4.3. *Let $K := K(n, \ell)$.*

(1) *For any $\alpha \in \mathbf{M}_4$, the density of $\mathfrak{p} \in \mathscr{P}_K^{2\ell}$ such that $\varphi(\mathfrak{p}) = \alpha$ is $\frac{1}{2^n}$. That is,*

$$d(\mathbf{r}_0^{-1}(\alpha) | \mathscr{P}_K^{2\ell}) = \frac{1}{\#\mathbf{M}_4} = \frac{1}{2^n}.$$

(2) *Furthermore, the density does not change when we restrict to primes of K that split completely in $K/\mathbb{Q}$. That is,*

$$d(\mathbf{r}_0^{-1}(\alpha) \cap S' | S') = \frac{1}{\#\mathbf{M}_4} = \frac{1}{2^n}.$$

Proof. Recall that $\mathrm{nR}^4 = \mathrm{nR}_K^4$ denotes the narrow ray class field over K of conductor $4\mathfrak{m}_\infty$. Let $G := \mathrm{Gal}(\mathrm{nR}^4 / K)$. Define $H \leq G$ to be

$$H := \mathrm{Art}(\ker(\varphi))$$

where Art denotes the Artin isomorphism. In other words, we define H by the following commutative diagram of exact sequences

$$\begin{tikzcd}
1 \arrow[r] & \ker(\varphi) \arrow[r] \arrow[d, "\mathrm{Art}"] & \mathrm{n}\mathcal{C}\mathrm{l}^4 \arrow[r, "\varphi"] \arrow[d, "\mathrm{Art}"] & \mathbf{M}_4 \arrow[r] \arrow[d, "\mathrm{id.}"] & 1 \\
1 \arrow[r] & H \arrow[r] & G \arrow[r] & \mathbf{M}_4 \arrow[r] & 1
\end{tikzcd}$$

where surjectivity of φ is proven in Lemma 3.5. Let L be the fixed field of H so that $\mathrm{Gal}(L/K) \cong G/H$.

$$\begin{tikzcd}
\mathrm{nR}^4 \arrow[d, dash] \arrow[d, bend right=60, dash, "H"'] \arrow[dd, bend left=60, dash, "G"] \\
L \arrow[d, dash] \\
K
\end{tikzcd}$$

This induces a canonical isomorphism

$$\mathbf{M}_4 \cong G/H \cong \mathrm{Gal}(L/K).$$

For $\alpha \in \mathbf{M}_4$, define $P(\alpha)$ to be the set of odd unramified prime ideals of K which map to α via φ. Let $\sigma \in G/H$ corresponding to α. Then

$$P(\alpha) = \{\mathfrak{p} \in \mathscr{P}_K^{2\ell} : \mathrm{Art}_{L|K}(\mathfrak{p}) = \sigma\}$$

where $\mathscr{P}_K^{2\ell}$ is the set of odd unramified prime ideals of K and $\mathrm{Art}_{L|K}$ denotes the Artin map for the extension $L|K$.

Theorem 4 in [Ser81] asserts Cebotarev's Density Theorem for natural density, (or see [Neu99] Theorem VII.13.4 for a simpler proof using Dirichlet density). By the special case of Cebotarev's Density Theorem in which L/K is cyclic, $P(\alpha)$ has a density and it is given by

$$\frac{1}{\#\,\mathrm{Gal}(L/K)} = \frac{1}{\#\mathbf{M}_4}.$$

The first asserted equality of part (1) is proved. The second equality of part (1) is true by Lemma 3.3.

To prove part (2), observe that

$$d(\mathbf{r}_0^{-1}(\alpha)|\mathscr{P}_K^{2\ell}) = d(\mathbf{r}_0^{-1}(\alpha)\cap S'|S')d(S'|\mathscr{P}_K^{2\ell}) + d(\mathbf{r}_0^{-1}(\alpha)\cap I'|I')d(I'|\mathscr{P}_K^{2\ell}).$$

Since $d(S'|\mathscr{P}_K^{2\ell}) = 1$, $d(I'|\mathscr{P}_K^{2\ell}) = 0$, and $0 \le d(\mathbf{r}_0^{-1}(\alpha)\cap I'|I') \le 1$,

$$d(\mathbf{r}_0^{-1}(\alpha)|\mathscr{P}_K^{2\ell}) = d(\mathbf{r}_0^{-1}(\alpha)\cap S'|S'). \quad \square$$

5. Property star and the starlight invariant

Let $K := K(n,\ell)$. Recall that $\mathbb{M}_{4,G}$ denotes the set of $\mathrm{Gal}(K/\mathbb{Q})$-orbits of $\mathbf{M}_4$ and recall the statement of Lemma 2.2, which motivates the following.

Theorem 5.1. *Let $K := K(n,\ell)$. Let $\alpha \in \mathcal{O}_K$ denote a representative of $[\alpha] \in \mathbb{M}_{4,G}$. Define the map*

$$\begin{aligned} \star : \mathbb{M}_{4,G} &\to \{\pm 1\} \\ [\alpha] &\mapsto \begin{cases} 1 & \text{if } (\alpha,\alpha^\sigma)_2 = 1 \text{ for all non-trivial } \sigma \in \mathrm{Gal}(K/\mathbb{Q}) \\ -1 & \text{otherwise.} \end{cases} \end{aligned}$$

Then $\star$ is a well-defined map.

Note that by Lemma 2.2, a rational prime p satisfies the spin relation

$$\mathrm{spin}(\mathfrak{p},\sigma) = \mathrm{spin}(\mathfrak{p},\sigma^{-1}) \quad \text{for all } \sigma \neq 1 \in \mathrm{Gal}(K/\mathbb{Q}),$$

where $\mathfrak{p}$ is a prime of K above p exactly when $\star \circ \mathbf{r}(p) = 1$ where $\mathbf{r}$ is as defined in Definition 3.4.

Proof. We will show that $\star$ is well-defined out of $\mathbf{M}_4$. Then because $\star$ is a property of the full Galois orbit, $\star$ is well-defined out of $\mathbb{M}_{4,G}$.

Let $\alpha, \beta \in \mathcal{O}_K$ be two representatives of the same class in $\mathbf{M}_4$ so

$$\alpha \equiv \beta\gamma^2 \bmod 4\mathcal{O}_K \quad \text{for some } \gamma \in \mathcal{O}_K.$$

If $\alpha \equiv \beta\gamma^2 \bmod 8\mathcal{O}_K$ then we can apply Lemma 2.3 from [FIMR13] to see that $(\alpha, \alpha^\sigma)_2 = (\beta, \beta^\sigma)_2$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Therefore, we may assume

$$\alpha \equiv 5\beta\gamma^2 \bmod 8\mathcal{O}_K.$$

Suppose $(\alpha, \alpha^\sigma)_2 = 1$. Then by Lemma 2.3 in [FIMR13], since $\alpha \equiv 5\beta\gamma^2 \bmod 8\mathcal{O}_K$,

$$\begin{aligned} &\left(5\beta\gamma^2, \left(5\beta\gamma^2\right)^\sigma\right)_2 = 1 \\ \implies &\left(5\beta, (5\beta)^\sigma\right)_2 = 1 \quad \text{by a property of Hilbert symbols.} \end{aligned}$$

Using bimultiplicativity of the Hilbert symbol,

$$\left(5\beta, (5\beta)^\sigma\right)_2 = (5,5)_2(\beta,5)_2(5,\beta^\sigma)_2(\beta,\beta^\sigma)_2.$$

Notice that since 2 is inert in $K/\mathbb{Q}$ and since 5 is invariant under the action of $\mathrm{Gal}(K/\mathbb{Q})$, applying the Galois action to the quadratic form for $(\beta, 5)_2$ yields the form for $(5, \beta^\sigma)_2$ so the cross terms cancel one another. Therefore

$$\left(5\beta, (5\beta)^\sigma\right)_2 = (5,5)_2(\beta,\beta^\sigma)_2.$$

Since $5 \times 2^2 + 5 \times 1^2 = 5^2$, $(5,5)_2 = 1$. Therefore

$$\left(5\beta, (5\beta)^\sigma\right)_2 = (\beta,\beta^\sigma)_2$$

so

$$(\alpha, \alpha^\sigma)_2 = 1 \implies (\beta, \beta^\sigma)_2 = 1.$$

Therefore $\star$ is a well-defined map from $\mathbf{M}_4$.

We now prove that if $\alpha, \beta \in \mathbf{M}_4$ are the in same Galois orbit, then $\star(\alpha) = \star(\beta)$. Let $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\alpha^\tau = \beta$ for $\alpha, \beta \in \mathbf{M}_4$.

Suppose $(\alpha, \alpha^\sigma)_2 = 1$ for all $\sigma \neq 1$ in $\mathrm{Gal}(K/\mathbb{Q})$. Then in $K_{(2)}$, the completion of K at $2\mathcal{O}_K$, there is a nontrivial solution x, y, z to

$$\alpha x^2 + \alpha^\sigma y^2 = z^2.$$

Applying the action of τ yields a nontrivial solution to

$$\beta x^2 + \beta^\sigma y^2 = z^2$$

so $(\beta, \beta^\sigma)_2 = 1$ for all $\sigma \neq 1$. $\square$

Recall that by Lemma 3.3, the elements of $\mathbf{M}_4$ that are invariant under the $\mathrm{Gal}(K/\mathbb{Q})$-action are exactly ± 1. The following lemma fully describes $\star$ on these invariants.

Lemma 5.2. *Let $K := K(n, \ell)$.*

(1) $\star(1) = 1$.
(2) $\star(-1) = -1$.

Proof. Observe that $(1,1)_2 = 1$ because $x^2 + y^2 = z^2$ has the solution $(x, y, z) = (1, 0, 1)$.

If $(-1,-1)_2 = 1$, there would be a non-trivial solution to $x^2 + y^2 + z^2 \equiv 0 \bmod 4$. Since there is no such solution, $(-1,-1)_2 = -1$. $\square$

Definition 5.3. Let $K := K(n, \ell)$. Define the *starlight invariant*, m_K to be the number of $\mathrm{Gal}(K/\mathbb{Q})$-orbits X of $\mathbf{M}_4$ of non-trivial size such that $\star(X) = 1$. That is, for σ a generator of $\mathrm{Gal}(K/\mathbb{Q})$,

$$m_K := \#\{X \in \mathbb{M}_{4,G} : \#X = n \text{ and } \star(X) = 1\}.$$

Remark 5.4. By Lemma 5.2, it is equivalent to define the *starlight invariant* of K, as

$$m_K = \#\ker(\star) - 1.$$

Here $\star$ refers to the map $\star : \mathbb{M}_{4,G} \to \pm 1$ given in Theorem 5.1.

We now define

$$\star : \mathscr{P}_K^2 \to \{\pm 1\} \quad \text{and} \quad \star : \mathscr{P}_{\mathbb{Q}}^2 \to \{\pm 1\}$$

to be the composition of $\star$ as defined in Theorem 5.1 with $\mathbf{r}_0$ and $\mathbf{r}$ respectively as defined in Definition 3.4.

Definition 5.5. Let $p \in \mathscr{P}_{\mathbb{Q}}^2$ and let $\mathfrak{p} \in \mathscr{P}_K^2$. Define $\star(\mathfrak{p}) := \star \circ \mathbf{r}_0$ and $\star(p) := \star \circ \mathbf{r}$, the composition of the maps $\mathbf{r}_0$ and $\mathbf{r}$ respectively with the map $\star$ from Definition 3.4.

We say that a prime $\mathfrak{p} \in \mathscr{P}_K^2$ (respectively $p \in \mathscr{P}_{\mathbb{Q}}^2$) has property $\star$ or that $\star$ is true for $\mathfrak{p}$ (respectively p) whenever $\star(\mathfrak{p}) = 1$ (respectively $\star(p) = 1$).

Theorem 6.2 and Theorem 1.2 give formulas in terms of n and m_K for the density of rational primes (assumed to split completely in Theorem 6.2) that satisfy property $\star$.

6. Density theorems

We first state and prove Theorem 6.2 which gives a formula describing the restricted density of rational primes that satisfy the spin relation, the restriction being to primes that split completely in $K/\mathbb{Q}$. Handling the inert case separately, we then apply Theorem 6.2 to obtain Theorem 1.2 which gives a formula for the overall density of rational primes that satisfy the given spin relation. Lastly, we prove Theorems 6.5 and 1.3 which give bounds on the densities given in Theorems 6.2 and 1.2 respectively.

Recall the definitions of S, S', I, and I' from Definition 4.2.

Definition 6.1. Let $K := K(n, \ell)$. Define the following sets of rational primes.

$$B := \{p \in \mathscr{P}_{\mathbb{Q}}^{2\ell} : \star(p) = 1\}$$
$$R := B \cap S.$$

Note that by Lemma 2.2, B is exactly the set of rational primes in $p \in \mathscr{P}_{\mathbb{Q}}^{2\ell}$ such that

$$\mathrm{spin}(\mathfrak{p}, \sigma) = \mathrm{spin}(\mathfrak{p}, \sigma^{-1}) \quad \text{for all } \sigma \in \mathrm{Gal}(K/\mathbb{Q})$$

where $\mathfrak{p}$ is a prime of K above p.

Recall from Definition 4.1 that $d(R|S)$ denotes the restricted density of primes $p \in R$ restricted to S.

Theorem 6.2. *Let $K := K(n, \ell)$. Then*

$$d(R|S) = \frac{1 + m_K n}{2^n}.$$

Proof. Let $N \in \mathbb{Z}_+$. Let R_N and S_N denote the sets of primes in R and S respectively of norm less than N. We will show that

$$\lim_{N\to\infty} \frac{\#R_N}{\#S_N} = \frac{\#\{X \in \mathbf{M}_4 : \star(X) = 1\}}{\#\mathbf{M}_4} = \frac{1 + m_K n}{2^n}. \tag{4}$$

Let $R'_N \subseteq \mathscr{P}_K^{2\ell}$ denote the set of primes of K that lay above rational primes in $R_N \subseteq \mathscr{P}_{\mathbb{Q}}^{2\ell}$ and define S'_N similarly with respect to $S_N \subseteq \mathscr{P}_{\mathbb{Q}}^{2\ell}$. Let $\mathbf{r}_{0,N}$ denote the restriction of $\mathbf{r}_0$ to $S'_N \subseteq \mathscr{P}_K^{2\ell}$. Since we have restricted to primes that split completely in $K/\mathbb{Q}$,

$$\frac{\#R_N}{\#S_N} = \frac{\#R'_N}{\#S'_N}$$

and

$$R'_N = \bigcup_{\star(\alpha)=1} \mathbf{r}_{0,N}^{-1}(\alpha)$$

where the above is a disjoint union over elements $\alpha \in \mathbf{M}_4$ such that $\star(\alpha) = 1$. Therefore

$$\frac{\#R'_N}{\#S'_N} = \frac{1}{\#S'_N} \sum_{\star(\alpha)=1} \#\mathbf{r}_{0,N}^{-1}(\alpha).$$

By Lemma 4.3, this implies

$$\begin{aligned}\lim_{N\to\infty} \frac{\#R'_N}{\#S'_N} &= \sum_{\star(\alpha)=1} \lim_{N\to\infty} \frac{\#\mathbf{r}_{0,N}^{-1}(X)}{\#S'_N} \\ &= \sum_{\star(\alpha)=1} \frac{1}{2^n} \\ &= \frac{\#\{\alpha \in \mathbf{M}_4 : \star(\alpha) = 1\}}{2^n}.\end{aligned}$$

This proves the first equality in equation 4. Let σ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$. By Lemma 3.3, the elements of $\alpha \in \mathbf{M}_4$ such that $\alpha^\sigma = \alpha$ are $\alpha = \pm 1$ and we know that $\star(1) = 1$ and $\star(-1) = -1$ by Lemma 5.2. Recalling that $m_K = \#\{[\alpha] \in \mathbb{M}_{4,G} : \alpha^\sigma \neq \alpha, \star(\alpha) = 1\}$, this implies

$$\#\{\alpha \in \mathbf{M}_4 : \star(\alpha) = 1\} = m_K n + 1,$$

since $n = [K : \mathbb{Q}]$ is prime so Galois orbits $X \in \mathbb{M}_{4,G}$ such that $X^\sigma \neq X$ each contain n elements. □

We now state an extended version of Lemma 4.3 which handles the inert case allowing us to give a formula in Theorem 1.2 for $d(B|\mathscr{P}_{\mathbb{Q}}^{2\ell})$, the overall density of rational primes that satisfy $\star$.

Lemma 6.3. *Let $K := K(n, \ell)$.*

(1) *For any $\alpha \in \mathbf{M}_4$, the density of $\mathfrak{p} \in \mathscr{P}_K^{2\ell}$ such that $\varphi(\mathfrak{p}) = \alpha$ is $\frac{1}{2^n}$. That is,*

$$d(\mathbf{r}_0^{-1}(\alpha)|\mathscr{P}_K^{2\ell}) = \frac{1}{\#\mathbf{M}_4} = \frac{1}{2^n}.$$

(2) *Restricting to primes of K that split completely in $K/\mathbb{Q}$,*

$$d(\mathbf{r}_0^{-1}(\alpha) \cap S'|S') = \frac{1}{\#\mathbf{M}_4} = \frac{1}{2^n}.$$

(3) *Restricting to inert primes of K,*

$$d(\mathbf{r}_0^{-1}(\alpha) \cap I'|I') = \begin{cases} \frac{1}{2} & \text{if } \alpha = \pm 1 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Part (a) and part (b) were proven in Lemma 4.3.

If $\alpha \neq \pm 1$ (for $\alpha \in \mathbf{M}_4$) then $\mathbf{r}_0^{-1}(\alpha) \cap I' = \emptyset$ since ± 1 are the only invariants of the $\mathrm{Gal}(K/\mathbb{Q})$-action on $\mathbf{M}_4$ by Lemma 3.3. Therefore $d(\mathbf{r}_0^{-1}(\alpha) \cap I'|I') = 0$ if $\alpha \neq \pm 1$.

Now fix $s = \pm 1$. Then

$$\mathbf{r}_0^{-1}(s) \cap I' = \left\{\mathfrak{p} \in I' : \left(\frac{\alpha}{4}\right)_K = s\right\}$$

where $\left(\frac{\alpha}{4}\right)_K$ denotes the quadratic residue symbol in $\mathcal{O}_K$ for $\alpha \in \mathcal{O}_K$ a totally positive generator of $\mathfrak{p}^{h(K)}$. The quadratic residue condition is a congruence condition modulo 4 and being inert is a congruence condition with an odd modulus so the Chinese remainder theorem together with the cyclic case of Cebotarev's Density Theorem implies

$$d(\mathbf{r}_0^{-1}(s) \cap I'|I') = \frac{1}{2}.$$

Theorem 4 in [Ser81] asserts Cebotarev's Density Theorem for natural density, or see [Neu99] Theorem VII.13.4 for an simpler proof using Dirichlet density. □

We now prove the main results.

Theorem 1.2. *Let $K := K(n, \ell)$. The density of rational primes p that satisfy the spin relation*

$$\mathrm{spin}(\mathfrak{p}, \sigma) = \mathrm{spin}(\mathfrak{p}, \sigma^{-1}) \quad \textit{for all } \sigma \neq 1 \in \mathrm{Gal}(K/\mathbb{Q})$$

where $\mathfrak{p}$ is a prime of K above p is given by

$$D_K = \frac{2^{n-1}(n-1) + m_K n + 1}{2^n n}.$$

Proof. Recall Definition 6.1. Note that by Lemma 2.2, B is the set of rational primes not dividing 2ℓ that satisfy the given spin relation. Therefore

$$D_K = d(B|\mathscr{P}_{\mathbb{Q}}^{2\ell}).$$

Let $N \in \mathbb{Z}_+$. Let I_N and S_N denote the sets of (rational) primes in I and S respectively with positive generator less than N. Let $I'_N \subseteq \mathscr{P}_K^{2\ell}$ denote the set of primes of K which lay above rational primes in $I_N \subseteq \mathscr{P}_{\mathbb{Q}}^{2\ell}$ and define S'_N similarly with respect to $S_N \subseteq \mathscr{P}_{\mathbb{Q}}^{2\ell}$. Note that while $S'_N = \{\mathfrak{p} \in S' : \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p}) < N\}$,

$$I'_N = \{\mathfrak{p} \in I' : \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{p}) < N^n\}.$$

Since we have restricted to primes that are inert in $K/\mathbb{Q}$,

$$\frac{\#B \cap I_N}{\#I_N} = \frac{\#B' \cap I'_N}{\#I'_N}$$

where $B' := \{\mathfrak{p} \in \mathscr{P}_K^{2\ell} : \star(\mathfrak{p}) = 1\} = \{\mathfrak{p} \in \mathscr{P}_K^{2\ell} : \mathfrak{p}$ lays above some $p \in B\}$.

Let $\mathbf{r}_{0,N}$ denote the restriction of $\mathbf{r}_0$ to $I'_N \subseteq \mathscr{P}_K^{2\ell}$. Observe that $\mathfrak{p} \in I'$ implies $\mathfrak{p}^\sigma = \mathfrak{p}$ so $\mathbf{r}_0(\mathfrak{p}) = \pm 1$ for all $\mathfrak{p} \in I'$ by Lemma 3.3. Lemma 5.2 states that $\star(1) = 1$ and $\star(-1) = -1$. Therefore

$$B' \cap I'_N = \mathbf{r}_0^{-1}(1) \cap I'_N.$$

Therefore $d(B' \cap I'|I') = \frac{1}{2}$ by part (c) of Lemma 6.3. Then since $\frac{\#B \cap I_N}{\#I_N} = \frac{\#B' \cap I'_N}{\#I'_N}$, we have proven that

$$d(B \cap I|I) = \frac{1}{2}. \tag{5}$$

Note that since $K/\mathbb{Q}$ is cyclic, $\mathscr{P}_\mathbb{Q}^{2\ell}$ is the disjoint union of S and I.

Cebotarev's Density Theorem is true for natural density by Theorem 4 in [Ser81]. (Theorem VII.13.4 in [Neu99] gives a simpler proof using Dirichlet density.)

By Cebotarev's Density Theorem, $d(S|\mathscr{P}_\mathbb{Q}^{2\ell}) = \frac{1}{n}$ and $d(I|\mathscr{P}_\mathbb{Q}^{2\ell}) = \frac{n-1}{n}$. Therefore

$$\begin{aligned} d(B|\mathscr{P}_\mathbb{Q}^{2\ell}) &= \lim_{N\to\infty} \frac{\#B_N}{\#\mathscr{P}_{\mathbb{Q},N}^{2\ell}} = \lim_{N\to\infty} \left(\frac{\#B \cap I_N}{\#I_N} \frac{\#I_N}{\#\mathscr{P}_{\mathbb{Q},N}^{2\ell}} + \frac{\#B \cap S_N}{\#S_N} \frac{\#S_N}{\#\mathscr{P}_{\mathbb{Q},N}^{2\ell}} \right) \\ &= \left(\frac{1}{2}\right)\left(\frac{n-1}{n}\right) + \left(\frac{m_K n + 1}{2^n}\right)\left(\frac{1}{n}\right) \quad \text{by Theorem 6.2} \\ &= \frac{2^{n-1}(n-1) + m_K n + 1}{2^n n}. \quad \square \end{aligned}$$

Lemma 6.4. *Let $K := K(n, \ell)$. For all $\alpha \in \mathbf{M}_4$, if $\star(\alpha) = 1$ then $\star(-\alpha) = -1$.*

Proof. By Lemma 5.2, $(-1, -1)_2 = -1$.

Next note that $(a, b)_2 = (a^\sigma, b^\sigma)_2$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ since 2 is inert in K.

Assume $\star(\alpha) = 1$. Then $(\alpha, \alpha^\sigma)_2 = 1$ for all nontrivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be nontrivial. By bimultiplicativity of Hilbert symbols,

$$\begin{aligned} (-\alpha, -\alpha^\sigma)_2 &= (-\alpha, -1)_2(-\alpha, \alpha^\sigma)_2 \\ &= (-1, -1)_2(\alpha, -1)_2(-1, \alpha^\sigma)_2(\alpha, \alpha^\sigma)_2. \end{aligned}$$

Next observe $(\alpha, -1)_2 = (-1, \alpha)_2 = (-1, \alpha^\sigma)_2$, the second equality coming from the Galois-invariance shown earlier in this proof. Therefore $(\alpha, -1)_2(-1, \alpha^\sigma)_2 = 1$. Then since $(\alpha, \alpha^\sigma)_2 = 1$ and $(-1, -1)_2 = -1$, we get that

$$(-\alpha, -\alpha^\sigma)_2 = -1.$$

Therefore $\star(-\alpha) = -1$. $\square$

Recall the Definitions 4.2 and 6.1 defining S and R.

Theorem 6.5. *Let $K := K(n, \ell)$.*

$$\frac{1}{2^n} \leq d(R|S) \leq \frac{1}{2}.$$

Proof. By Theorem 6.2,

$$d(R|S) = \frac{1 + m_K n}{2^n} = \frac{\#\{\alpha \in \mathbf{M}_4 : \star(\alpha) = 1\}}{2^n}.$$

Lemma 6.4 implies the upper bound; $\alpha \neq -\alpha$ in $\mathbf{M}_4$ because -1 is not a square modulo $4\mathcal{O}_K$.

The lower bound is true because $\star(1) = 1$ by Lemma 5.2 so

$$\#\{\alpha \in \mathbf{M}_4 : \star(\alpha) = 1\} \geq 1. \quad \square$$

Theorem 1.3 is a Corollary of Theorem 6.5 obtained from the fact that

$$D_K = \frac{n-1}{2n} + \left(\frac{1}{n}\right) d(R|S)$$

as in the proof of Theorem 1.2.

Theorem 1.3. *Let $K := K(n, \ell)$. Then*

$$0 < \frac{2^{n-1}(n-1)+1}{2^n n} \leq D_K \leq \frac{1}{2}.$$

Acknowledgments

This research was conducted at Cornell University under the supervision of Ravi Ramakrishna. The paper was finalized at the Max Planck Institute for Mathematics. In addition, the author would like to thank Brian Hwuang, Christian Maire, and Carlo Pagano for their helpful mathematical discussions, and Pieter Moree for his guidance.

References

[AF67] J.V. Armitage, A. Fröhlich, Classnumbers and unit signatures, Mathematika 14 (1967) 94–98.

[BCP97] Wieb Bosma, John Cannon, Catherine Playoust, The magma algebra system. I. The user language, J. Symbolic Comput. 24 (3–4) (1997) 235–265, Computational Algebra and Number Theory (London, 1993).

[FIMR13] J.B. Friedlander, H. Iwaniec, B. Mazur, K. Rubin, The spin of prime ideals, Invent. Math. 193 (3) (2013) 697–749.

[McM18] Christine McMeekin, A Density of Ramified Primes, ProQuest LLC, Ann Arbor, MI, 2018, Thesis (Ph.D.)–Cornell University.

[Mil13] J.S. Milne, Class Field Theory (v4.02), 2013, available at www.jmilne.org/math/.
[Mun] Sam Mundy, Conversation.
[Neu99] Jürgen Neukirch, Algebraic Number Theory, Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences), vol. 322, Springer-Verlag, Berlin, 1999, translated from the 1992 German original and with a note by Norbert Schappacher, with a foreword by G. Harder.
[Ser81] Jean-Pierre Serre, Quelques applications du théorème de densité de Chebotarev, Publ. Math. Inst. Hautes Études Sci. (54) (1981) 323–401.