A density of ramified primes

Stephanie Chan

University of Michigan

Spins

Given a number field K, let $\mathcal{O}_{K,+}^{\times} := \{u \in \mathcal{O}_K^{\times} : u \text{ totally positive}\}$.

Friedlander, Iwaniec, Mazur, and Rubin studied, in number fields K satisfying

(P1) $K/\mathbb{Q}$ is Galois, K is totally real, $\mathcal{O}_{K,+}^{\times} = \left(\mathcal{O}_K^{\times}\right)^2$, and

(P2) $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic,

the behaviour of a quadratic residue symbol defined on any odd **principal** ideal $\mathfrak{a}$ and any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$,

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

where α is any totally positive generator of $\mathfrak{a}$.

Spins

Given a number field K, let $\mathcal{O}_{K,+}^{\times} := \{u \in \mathcal{O}_K^{\times} : u \text{ totally positive}\}$.

Friedlander, Iwaniec, Mazur, and Rubin studied, in number fields K satisfying

(P1) $K/\mathbb{Q}$ is Galois, K is totally real, $\mathcal{O}_{K,+}^{\times} = \left(\mathcal{O}_K^{\times}\right)^2$, and

(P2) $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic,

the behaviour of a quadratic residue symbol defined on any odd **principal** ideal $\mathfrak{a}$ and any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$,

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

where α is any totally positive generator of $\mathfrak{a}$.

The assumption $\mathcal{O}_{K,+}^{\times} = \left(\mathcal{O}_K^{\times}\right)^2$ ensures that

- any principal ideal has a totally positive generator ($\mathcal{O}_{K,+}^{\times} = \left(\mathcal{O}_K^{\times}\right)^2$ if and only if $\mathrm{Cl}^+ = \mathrm{Cl}$, when K is totally real);
- any two totally positive generators of $\mathfrak{a}$ differ by a square, so the spin is independent of the choice of totally positive generator α.

Some applications of spins

- 2-Selmer group of elliptic curves (Friedlander–Iwaniec–Mazur–Rubin).

Example (Friedlander–Iwaniec–Mazur–Rubin)

Let $E : y^2 = x^3 + x^2 - 16x - 29$ and $K = \mathbb{Q}(E[2])$. Then K is a cyclic extension of $\mathbb{Q}$ of degree 3. Take σ to be a generator of $\mathrm{Gal}(K/\mathbb{Q})$. If p is a rational prime that splits completely in K, and a prime $\mathfrak{p}$ above p has a totally positive generator congruent to 1 mod 8, then

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E^{(p)}) = \begin{cases} 3 & \text{if } \mathrm{spin}(\mathfrak{p}, \sigma) = 1 \\ 1 & \text{if } \mathrm{spin}(\mathfrak{p}, \sigma) = -1. \end{cases}$$

- 16-rank of class groups of quadratic fields (Koymans–Milovic).

Distribution of spins

Friedlander, Iwaniec, Mazur, and Rubin proved that if σ is a (fixed) generator of $\mathrm{Gal}(K/\mathbb{Q})$, the density of principal prime ideals $\mathfrak{p}$ in K such that $\mathrm{spin}(\mathfrak{p}, \sigma) = 1$ is equal to $1/2$, conditional to the following conjecture.

Conjecture C_η

Let η be a real number satisfying $0 < \eta \leq 1$. Then there exists a real number $\delta = \delta(\eta) > 0$ such that for all $\epsilon > 0$ there exists a real number $C = C(\eta, \epsilon) > 0$ such that for all integers $Q \geq 3$, all real non-principal characters χ of conductor $q \leq Q$, all integers $N \leq Q^\eta$, and all integers M, we have

$$\left| \sum_{M < a \leq M+N} \chi(a) \right| \leq C Q^{\eta(1-\delta)+\epsilon}.$$

A conjecture on short character sums

Conjecture C_η

Let η be a real number satisfying $0 < \eta \leq 1$. Then there exists a real number $\delta = \delta(\eta) > 0$ such that for all $\epsilon > 0$ there exists a real number $C = C(\eta, \epsilon) > 0$ such that for all integers $Q \geq 3$, all real non-principal characters χ of conductor $q \leq Q$, all integers $N \leq Q^\eta$, and all integers M, we have

$$\left| \sum_{M < a \leq M+N} \chi(a) \right| \leq C Q^{\eta(1-\delta)+\epsilon}.$$

Conjecture C_η is

- known for $\eta > 1/4$, as a consequence of the classical Burgess's inequality;
- open for $\eta \leq 1/4$;
- for sums as above starting at $M = 0$, a consequence of the Generalised Riemann Hypothesis for the L-function $L(s, \chi)$.

Theorem (Friedlander–Iwaniec–Mazur–Rubin)

Suppose K is a totally real number field, cyclic Galois over $\mathbb{Q}$, and satisfying $\mathcal{O}_{K,+}^{\times} = \left(\mathcal{O}_K^{\times}\right)^2$. Suppose $n = [K : \mathbb{Q}] \geq 3$. Assume Conjecture C_η holds for $\eta = \frac{1}{n}$ with $\delta = \delta(\eta) > 0$. Let σ be a generator of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. Then for all $X > 3$, we have

$$\left| \sum_{\substack{\mathfrak{p} \text{ principal} \\ \mathrm{Norm}(\mathfrak{p}) \leq X}} \mathrm{spin}(\mathfrak{p}, \sigma) \right| \ll_{\epsilon, K} X^{1-\theta+\epsilon}$$

where $\theta = \theta(n) = \frac{\delta}{2n(12n+1)}$.

The result still holds when congruence conditions are imposed.

The proof uses Vinogradov's method of sums of type I and type II.

By Burgess's inequality, Conjecture C_η holds for $\eta = 1/3$ with $\delta = \frac{1}{48}$, so the theorem holds unconditionally for $[K : \mathbb{Q}] = 3$ where $\theta = \frac{1}{10656}$.

Joint distribution of spins

Given $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\}$ such that $\sigma \neq \tau$ and $\sigma \neq \tau^{-1}$, Koymans and Milovic proved that $\mathrm{spin}(\mathfrak{p}, \sigma)$ and $\mathrm{spin}(\mathfrak{p}, \tau)$ are distributed independently, i.e. that the product $\mathrm{spin}(\mathfrak{p}, \sigma)\,\mathrm{spin}(\mathfrak{p}, \tau)$ oscillates (still conditional on Conjecture C_η).

Joint distribution of spins

Given $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\}$ such that $\sigma \neq \tau$ and $\sigma \neq \tau^{-1}$, Koymans and Milovic proved that $\mathrm{spin}(\mathfrak{p}, \sigma)$ and $\mathrm{spin}(\mathfrak{p}, \tau)$ are distributed independently, i.e. that the product $\mathrm{spin}(\mathfrak{p}, \sigma)\,\mathrm{spin}(\mathfrak{p}, \tau)$ oscillates (still conditional on Conjecture C_η).

More generally, they prove that the product of spins

$$\prod_{\sigma \in H} \mathrm{spin}(\mathfrak{p}, \sigma)$$

oscillates as long as the fixed non-empty $H \subset \mathrm{Gal}(K/\mathbb{Q})$ satisfies the property

$$\sigma \notin H \text{ whenever } \sigma^{-1} \in H.$$

Their result holds for number fields K satisfying

(P1) $K/\mathbb{Q}$ is Galois, K is totally real, $\mathcal{O}_{K,+}^{\times} = \left(\mathcal{O}_K^{\times}\right)^2$.

(not necessarily cyclic)

Theorem (Koymans–Milovic)

Suppose K is a totally real number field, Galois over $\mathbb{Q}$, and satisfying $\mathcal{O}_{K,+}^\times = \left(\mathcal{O}_K^\times\right)^2$. Suppose $H \subset \mathrm{Gal}(K/\mathbb{Q})$ is nonempty and satisfies the property

$$\sigma \notin H \text{ whenever } \sigma^{-1} \in H.$$

Suppose $n = [K : \mathbb{Q}] \geq 3$. Assume Conjecture C_η holds for $\eta = \frac{1}{n|H|}$ with $\delta = \delta(\eta) > 0$. Then for all $X > 3$, we have

$$\left| \sum_{\substack{\mathfrak{p} \text{ principal} \\ \mathrm{Norm}(\mathfrak{p}) \leq X}} \prod_{\sigma \in H} \mathrm{spin}(\mathfrak{p}, \sigma) \right| \ll_{\epsilon,K} X^{1-\theta+\epsilon}$$

where $\theta = \theta(n, |H|) = \frac{\delta}{54|H|^2 n(12n+1)}$.

The relation between some spins

The assumption $\sigma \notin H$ whenever $\sigma^{-1} \in H$ is made because $\text{spin}(\mathfrak{p}, \sigma)$ and $\text{spin}(\mathfrak{p}, \sigma^{-1})$ are not independent.

Lemma (Friedlander–Iwaniec–Mazur–Rubin)

Suppose K is a totally real number field, cyclic Galois over $\mathbb{Q}$, and satisfying $\mathcal{O}_{K,+}^{\times} = (\mathcal{O}_K^{\times})^2$. Suppose $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal and $\sigma \in \text{Gal}(K/\mathbb{Q})$ is such that $\mathfrak{p}$ and $\mathfrak{p}^{\sigma}$ are coprime. Then

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

where α is a totally positive generator of $\mathfrak{p}$.

This lemma is a consequence of Hilbert reciprocity and the fact that $(\alpha, \alpha^{\sigma})_{\mathfrak{p}} = \text{spin}(\mathfrak{p}, \sigma^{-1})$ and $(\alpha, \alpha^{\sigma})_{\mathfrak{p}^{\sigma}} = \text{spin}(\mathfrak{p}, \sigma)$.

Spins for non-principal ideals

We study the joint distribution of multiple spins $\text{spin}(\mathfrak{p}, \sigma)$, $\sigma \in H = \text{Gal}(K/\mathbb{Q}) \setminus \{1\}$, so there are many $\sigma \in H$ such that $\sigma^{-1} \in H$ as well.

Spins for non-principal ideals

We study the joint distribution of multiple spins $\mathrm{spin}(\mathfrak{p}, \sigma)$, $\sigma \in H = \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\}$, so there are many $\sigma \in H$ such that $\sigma^{-1} \in H$ as well.

Assuming the class number is odd, we can naturally extend the definition of spin to **all** odd ideals, not necessarily principal.

Definition

Suppose K is a cyclic Galois totally real number field satisfying $\mathcal{O}_{K,+}^{\times} = \left(\mathcal{O}_K^{\times}\right)^2$ and has odd class number. Given an odd ideal $\mathfrak{a}$, define the spin of $\mathfrak{a}$ with respect to $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ to be

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

where α is any totally positive generator of the principal ideal $\mathfrak{a}^h$.

We consider number fields K satisfying the following properties:

(P1) $K/\mathbb{Q}$ is Galois, K is totally real, $\mathcal{O}_{K,+}^{\times} = \left(\mathcal{O}_K^{\times}\right)^2$;

(P2) $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic;

(P3) the class number $\#\,\mathrm{Cl}$ of K is odd;

(P4) $n := [K : \mathbb{Q}]$ is odd; and

(P5) the prime 2 is inert in $K/\mathbb{Q}$.

We consider number fields K satisfying the following properties:

(P1) $K/\mathbb{Q}$ is Galois, K is totally real, $\mathcal{O}_{K,+}^{\times} = \left(\mathcal{O}_K^{\times}\right)^2$;

(P2) $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic;

(P3) the class number $\#\,\mathrm{Cl}$ of K is odd;

(P4) $n := [K : \mathbb{Q}]$ is odd; and

(P5) the prime 2 is inert in $K/\mathbb{Q}$.

The conditions are equivalent to

(C1) $K/\mathbb{Q}$ is Galois;

(C2) $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic;

(C3) the narrow class number $\#\,\mathrm{Cl}^{+}$ of K is odd;

(C4) $n := [K : \mathbb{Q}]$ is odd; and

(C5) the prime 2 is inert in $K/\mathbb{Q}$,

since (C1)+(C3)+(C4) implies (P1).

Density of primes satisfying a property of spins

Define $S := \{p \text{ prime} : p \text{ splits completely in } K/\mathbb{Q}\},$

$$F := \{p \in S : \mathrm{spin}(\mathfrak{p}, \sigma) = 1 \text{ for all } \sigma \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\}\},$$

where $\mathfrak{p}$ denotes a prime ideal in K lying above p.

Notice that $p \in F$

$$\Leftrightarrow \quad \mathfrak{p}^\sigma \text{ splits in } K(\sqrt{\alpha})/K \text{ for all } \sigma \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\}$$

$$\Leftrightarrow \quad \mathfrak{p} \text{ splits in } K(\sqrt{\alpha^\sigma})/K \text{ for all } \sigma \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\},$$

where α is a totally positive generator of the ideal $\mathfrak{p}^h$.

Density of primes satisfying a property of spins

Define $S := \{p \text{ prime} : p \text{ splits completely in } K/\mathbb{Q}\},$

$$F := \{p \in S : \text{spin}(\mathfrak{p}, \sigma) = 1 \text{ for all } \sigma \in \text{Gal}(K/\mathbb{Q}) \setminus \{1\}\},$$

where $\mathfrak{p}$ denotes a prime ideal in K lying above p.

Notice that $p \in F$

$$\Leftrightarrow \quad \mathfrak{p}^{\sigma} \text{ splits in } K(\sqrt{\alpha})/K \text{ for all } \sigma \in \text{Gal}(K/\mathbb{Q}) \setminus \{1\}$$

$$\Leftrightarrow \quad \mathfrak{p} \text{ splits in } K(\sqrt{\alpha^{\sigma}})/K \text{ for all } \sigma \in \text{Gal}(K/\mathbb{Q}) \setminus \{1\},$$

where α is a totally positive generator of the ideal $\mathfrak{p}^{h}$.

For sets of primes $A \subseteq B$, we define the restricted density

$$d(A|B) := \lim_{N \to \infty} \frac{\#\{p \in A : p < N\}}{\#\{p \in B : p < N\}}.$$

Goal: Find $d(F|S)$.

If the spins of a fixed prime ideal $\mathrm{spin}(\mathfrak{p}, \sigma)$ and $\mathrm{spin}(\mathfrak{p}, \tau)$ were independent for all $\sigma \neq \tau \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\}$, then one might expect the density of F restricted to S to be $2^{-(n-1)}$.

However, the relation

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

means that the density is not as straightforward.

Table: Densities computed for K of degree n satisfying the necessary hypotheses.

n	$d(F\|S)$	$1/2^{n-1}$	$2^{n-1}d(F\|S)$
3	1/4	1/4	1
5	3/64	1/16	0.75
7	11/512	1/64	1.375
9	7/2048	1/256	0.875
11	17/32768	1/1024	0.53125
13	33/262144	1/4096	0.51563
15	47/262144	1/16384	2.9375
17	145/16777216	1/65536	0.56640
19	257/134217728	1/262144	0.50195

Table: Densities computed for K of degree n satisfying the necessary hypotheses.

n	$d(F\|S)$	$1/2^{n-1}$	$2^{n-1}d(F\|S)$	order of 2 in $(\mathbb{Z}/n\mathbb{Z})^\times$
3	1/4	1/4	1	2
5	3/64	1/16	0.75	4
7	11/512	1/64	1.375	3
9	7/2048	1/256	0.875	6
11	17/32768	1/1024	0.53125	10
13	33/262144	1/4096	0.51563	12
15	47/262144	1/16384	2.9375	4
17	145/16777216	1/65536	0.56640	8
19	257/134217728	1/262144	0.50195	18

Theorem (C.–McMeekin–Milovic)

Let K be a cyclic number field of odd degree n over $\mathbb{Q}$ with odd narrow class number, and such that 2 is inert in $K/\mathbb{Q}$. Assume Conjecture C_η holds for $\eta = \frac{2}{n(n-1)}$. For $k \neq 1$ dividing n, let d_k be the order of 2 in $(\mathbb{Z}/k\mathbb{Z})^\times$. Then

$$d(F|S) = \frac{s_+ + s_-}{2^{(3n-1)/2}}$$

where

$$s_+ := 1 + \prod_{\substack{k|n,\ k\neq 1 \\ d_k\, odd}} 2^{\frac{\phi(k)}{2d_k}} \left(\prod_{\substack{k|n,\ k\neq 1 \\ d_k\, odd}} 2^{\frac{\phi(k)}{2}} - 1 \right),$$

and

$$s_- := \prod_{\substack{k|n,\ k\neq 1 \\ d_k\, even}} (2^{\frac{d_k}{2}} + 1)^{\frac{\phi(k)}{d_k}} \prod_{\substack{k|n,\ k\neq 1 \\ d_k\, odd}} (2^{d_k} - 1)^{\frac{\phi(k)}{2d_k}},$$

where ϕ denotes the Euler's totient function.

The cubic case is unconditional due to Burgess's inequality.

In particular, when $n = p$ is prime, writing d as the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$, we have

$$(s_+, s_-) = \begin{cases} \left(1 + 2^{\frac{p-1}{2d}}(2^{\frac{p-1}{2}} - 1),\ (2^d - 1)^{\frac{p-1}{2d}}\right) & \text{if } d \text{ is odd,} \\ \left(1,\ (2^{\frac{d}{2}} + 1)^{\frac{p-1}{d}}\right) & \text{if } d \text{ is even.} \end{cases}$$

When $d = p - 1$,

$$s_+ + s_- = 2^{\frac{p-1}{2}} + 2,$$

$$d(F|S) = \frac{s_+ + s_-}{2^{\frac{3p-1}{2}}} = \frac{1 + 2^{-\frac{p-1}{2}}}{2^p} \approx \frac{1}{2^p}.$$

Splitting up the density

Recall $S := \{p \text{ prime} : p \text{ splits completely in } K/\mathbb{Q}\},$

$F := \{p \in S : \mathrm{spin}(\mathfrak{p}, \sigma) = 1 \text{ for all } \sigma \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\}\},$

Define

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

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

Since $F \subseteq R \subseteq S$, if the limits exist then

$$d(F|S) = d(F|R)d(R|S).$$

Splitting up the density

Recall $S := \{p \text{ prime} : p \text{ splits completely in } K/\mathbb{Q}\}$,

$F := \{p \in S : \text{spin}(\mathfrak{p}, \sigma) = 1 \text{ for all } \sigma \in \text{Gal}(K/\mathbb{Q}) \setminus \{1\}\}$,

Define

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

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

Since $F \subseteq R \subseteq S$, if the limits exist then

$$d(F|S) = d(F|R)d(R|S).$$

Proving the density

$$d(F|R) = 2^{-\frac{n-1}{2}},$$

requires a modification of previous result by Koymans and Milovic.

The Hilbert symbol condition

We want to find $d(R|S)$.

Define a map $\star : S \to \{\pm 1\}$, such that

$$R = \{p \in S : \mathrm{spin}(\mathfrak{p}, \sigma) = \mathrm{spin}(\mathfrak{p}, \sigma^{-1}) \text{ for all } \sigma \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\}\}$$
$$= \{p \in S : \star(p) = 1\}.$$

With

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

we know that

$$\star(p) = 1 \text{ if and only if } (\alpha, \alpha^{\sigma})_2 = 1 \text{ for all } \sigma \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\},$$

where α is a totally positive generator of the ideal $\mathfrak{p}^h$.

The extra assumptions on K provide the following convenience:

- $\mathrm{Gal}(K/\mathbb{Q})$ being cyclic allows us to restrict to one generator,
- 2 being inert means the product $\prod_{v|2} (\alpha, \alpha^{\sigma})_v$ is simply $(\alpha, \alpha^{\sigma})_2$;
- $[K : \mathbb{Q}]$ being odd avoids involutions in $\mathrm{Gal}(K/\mathbb{Q})$.

The Hilbert symbol $(\cdot,\cdot)_2$, when restricted to odd primes, factors through $\mathbf{M}_4 := (\mathcal{O}_K/4\mathcal{O}_K)^\times/((\mathcal{O}_K/4\mathcal{O}_K)^\times)^2$ (viewed as a multiplicative group), so $\star(p)$ only depends on the class of $\mathfrak{p}$ in $\mathbf{M}_4$.

As an $\mathbb{F}_2$-vector space,

$$\mathbf{M}_4 = (\mathcal{O}_K/4\mathcal{O}_K)^\times/((\mathcal{O}_K/4\mathcal{O}_K)^\times)^2 \cong \mathcal{O}_K/2\mathcal{O}_K \cong (\mathbb{Z}/2\mathbb{Z})^n.$$

By the Chebotarev Density Theorem,

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

where $[\alpha]$ denotes the image of $\alpha \in \mathcal{O}_K$ in $\mathbf{M}_4$, and

$$\star(\alpha) = 1 \Leftrightarrow (\alpha, \alpha^\sigma)_2 = 1 \text{ for all } \sigma \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\}.$$

We want to find the number of elements in $\mathbf{M}_4$ with a representative $\alpha \in \mathcal{O}_K$ satisfying

$$(\alpha, \alpha^{\sigma})_2 = 1 \text{ for all } \sigma \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\}.$$

There exists some $y \in \mathcal{O}_K$ such that

$$\{[y^{\sigma}] : \sigma \in \mathrm{Gal}(K/\mathbb{Q})\} \text{ is a basis for } \mathbf{M}_4.$$

Fixing a generator σ of $\mathrm{Gal}(K/\mathbb{Q})$,

$$\mathbf{M}_4 = \left\{ \prod_{i=0}^{n-1} [y_{(i)}]^{u_i} : (u_0, \ldots, u_{n-1}) \in \mathbb{F}_2^n \right\}, \text{ where } y_{(i)} := y^{\sigma^i}.$$

The Hilbert symbol $(\cdot,\cdot)_2$ on $\mathbf{M}_4$ is

- multiplicatively bilinear,
- symmetric,
- non-degenerate,

so with respect to the basis $[y_{(i)}]$, $0 \le i \le n-1$, its matrix representation A is an $n \times n$ matrix over $\mathbb{F}_2$, that is symmetric and invertible.

The (i,j)-entry of A satisfies

$$(-1)^{A_{ij}} = (y_{(i)}, y_{(j)})_2.$$

For any $\mathbf{u} = (u_0, \ldots, u_{n-1}), \mathbf{v} = (v_0, \ldots, v_{n-1}) \in \mathbb{F}_2^n$, we have

$$\left(\prod_i y_{(i)}^{u_i}, \prod_j y_{(j)}^{v_j}\right)_2 = (-1)^{\mathbf{u}^T A \mathbf{v}}.$$

Define the $n \times n$ upper shift $\mathbb{F}_2$-matrix

$$T_1 := \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}, \quad T_k := T_1^k.$$

Then $\alpha = \prod_i y_{(i)}^{u_i}$, $\mathbf{u} = (u_0, \dots, u_{n-1}) \in \mathbb{F}_2^n$ satisfies

$$(\alpha, \alpha^\sigma)_2 = 1 \text{ for all } \sigma \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{1\}$$

$$\Leftrightarrow \qquad \mathbf{u}^T A T_1 \mathbf{u} = \mathbf{u}^T A T_2 \mathbf{u} = \dots = \mathbf{u}^T A T_{n-1} \mathbf{u} = 0,$$

$$\Leftrightarrow \qquad A \begin{pmatrix} \mathbf{u}^T T_0 \mathbf{u} \\ \mathbf{u}^T T_1 \mathbf{u} \\ \vdots \\ \mathbf{u}^T T_{n-1} \mathbf{u} \end{pmatrix} \in \left\{ \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right\}.$$

There is the following one-to-one correspondence

$$\Psi : \mathbb{F}_2^n \to \mathbb{F}_2[x]/(x^n - 1)$$
$$\mathbf{u} = (u_0, \ldots, u_{n-1}) \mapsto F_{\mathbf{u}}(x) = u_0 + u_1 x + u_2 x^2 + \cdots + u_{n-1} x^{n-1}.$$

The map

$$B : \ \mathbb{F}_2[x]/(x^n - 1) \to \mathbb{F}_2[x]/(x^n - 1)$$
$$F \mapsto x^n \cdot F(x)F(1/x).$$

fits into

$$\begin{array}{ccc} \mathbf{u} = (u_0, \ldots, u_{n-1}) & \overset{\Psi}{\longmapsto} & F_{\mathbf{u}}(x) \\ \downarrow & & \downarrow B \\ \mathbf{v} = (\mathbf{u}^T T_0 \mathbf{u},\ \mathbf{u}^T T_1 \mathbf{u},\ \ldots,\ \mathbf{u}^T T_{n-1} \mathbf{u}) & \overset{\Psi}{\longmapsto} & F_{\mathbf{v}}(x) = x^n \cdot F_{\mathbf{u}}(x) F_{\mathbf{u}}(1/x) \end{array}$$

Then

$$A \begin{pmatrix} \mathbf{u}^T T_0 \mathbf{u} \\ \mathbf{u}^T T_1 \mathbf{u} \\ \vdots \\ \mathbf{u}^T T_{n-1} \mathbf{u} \end{pmatrix} \in \left\{ \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right\}.$$

if and only if

$$B(F_{\mathbf{u}}) \in \{0, h(x)\},$$

where $h(x) = \Psi(A^{-1}(1, 0, \ldots, 0))$.

Lemma

$$\begin{aligned} &\#\{[\alpha] \in \mathbf{M}_4 : \star(\alpha) = 1\} \\ &= \#B^{-1}(0) + \#B^{-1}(h(x)) \\ &= \#\left\{F \in \mathbb{F}_2[x]/(x^n - 1) : x^n \cdot F(x)F(1/x) \equiv 0 \textit{ or } h(x)\right\}. \end{aligned}$$

We want to find formulas for $\#B^{-1}(0)$ and $\#B^{-1}(h(x))$.

Any F in

$$B^{-1}(0) = \{F \in \mathbb{F}_2[x]/(x^n - 1) : x^n \cdot F(x)F(1/x) \equiv 0\},$$

satisfy

$$(x^n - 1) \mid F(x)F^*(x),$$

where F^* denote the reciprocal of F, i.e. $F^*(x) = x^{\deg F} \cdot F(1/x)$.
Thus $\#B^{-1}(0)$ depends on the factorisation of $x^n - 1$ in $\mathbb{F}_2[x]$.

Any F in

$$B^{-1}(0) = \{F \in \mathbb{F}_2[x]/(x^n - 1) : x^n \cdot F(x)F(1/x) \equiv 0\},$$

satisfy

$$(x^n - 1) \mid F(x)F^*(x),$$

where F^* denote the reciprocal of F, i.e. $F^*(x) = x^{\deg F} \cdot F(1/x)$.
Thus $\#B^{-1}(0)$ depends on the factorisation of $x^n - 1$ in $\mathbb{F}_2[x]$.

$$x^3 - 1 = (x+1)(x^2 + x + 1)$$
$$x^5 - 1 = (x+1)(x^4 + x^3 + x^2 + x + 1)$$
$$x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

Lemma

For any factor $k \neq 1$ of n, let d_k be the order of 2 in $(\mathbb{Z}/k\mathbb{Z})^{\times}$. Also set $d_1 = 1$. Consider the following factorisation in $\mathbb{F}_2[x]$,

$$x^n - 1 = f_1(x) \dots f_r(x) f_{m+1}^*(x) \dots f_r^*(x), \tag{2}$$

where f_i are irreducible and $f_i = f_i^*$ for $i = 1, \dots, m$. Then $\sum_{i=1}^{r} \deg f_i = \sum_{k|n} r_k d_k$ and $r = \sum_{k|n} r_k$ and $m = \sum_{k|n} m_k$, where $r_1 = m_1 = 1$, and

$$(r_k, m_k) = \begin{cases} \left(\frac{\phi(k)}{2d_k},\ 0\right) & \text{if } d_k \text{ is odd,} \\ \left(\frac{\phi(k)}{d_k},\ \frac{\phi(k)}{d_k}\right) & \text{if } d_k \text{ is even,} \end{cases}$$

for $k \neq 1$.

Proposition

For each $k \neq 1$ dividing n, let d_k be the order of 2 in $(\mathbb{Z}/k\mathbb{Z})^\times$. Then

$$s_+ = 1 + \prod_{k|n,\ d_k \text{odd},\ k\neq 1} 2^{\frac{\phi(k)}{2d_k}} \left(\prod_{k|n,\ d_k \text{odd},\ k\neq 1} 2^{\frac{\phi(k)}{2}} - 1 \right),$$

and

$$s_- = \prod_{k|n,\ d_k \text{even},\ k\neq 1} (2^{d_k/2} + 1)^{\frac{\phi(k)}{d_k}} \prod_{k|n,\ d_k \text{odd},\ k\neq 1} (2^{d_k} - 1)^{\frac{\phi(k)}{2d_k}},$$

where ϕ denotes the Euler's totient function.

If $n = p$ is a prime, then writing d as the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$,

$$(s_+, s_-) = \begin{cases} \left(1 + 2^{\frac{p-1}{2d}} (2^{\frac{p-1}{2}} - 1),\ (2^d - 1)^{\frac{p-1}{2d}}\right) & \text{if } d \text{ is odd,} \\ \left(1,\ (2^{\frac{d}{2}} + 1)^{\frac{p-1}{d}}\right) & \text{if } d \text{ is even.} \end{cases}$$

In particular, when $n = 3$, $s_+ = 1$ and $s_- = 3$.

Thank you!