A Density of Ramified Primes

Christine McMeekin

Max Planck Institute for Mathematics
PhD, Cornell University

CIRM, 6th International Conference on Uniform Distribution Theory, October 2018

Motivation

Let $K(p)$ be a number field depending on a rational prime p (fixing the isomorphism class of $\mathrm{Gal}(K(p)/\mathbb{Q})$).

What is the density of rational primes p that exhibit a prescribed factorization in $K(p)/\mathbb{Q}$?

(Non-Interesting) Examples:

1. $K(p) := \mathbb{Q}(\sqrt{p})$.
2. Let $K(p) \subseteq \mathbb{Q}(\zeta_p)$ such that $[K(p) : \mathbb{Q}] = 3$ where we restrict to $p \equiv 1 \bmod 3$.

In both of these examples, p is totally ramified in $K(p)$ with density 1.

Summary

[McMng] For cyclic totally real number fields K of odd prime degree n satisfying certain assumptions, a spin dependence relation occurs with density given by a formula depending on n and m_K, a computable and bounded invariant of the number field K.

[McM18] A consequence of this result is a (conditional) theorem giving a formula for the density of rational primes exhibiting a prescribed (ramified) factorization in a number field depending on the prime in question. This density is strictly between 0 and 1.

Fix a Number Field K.

We now construct our family of number fields $K(p)$. First, we fix a number field K.

Let n be an odd prime and let $\ell \in \mathbb{Z}_+$ such that $\ell \equiv 1 \bmod n$. Let $K \subseteq \mathbb{Q}(\zeta_\ell)$ such that $[K : \mathbb{Q}] = n$. Note that such a cyclic number field is totally real. Assume the following.

1. K has odd class number.
2. Every totally positive unit of K is a square.
3. (for simplicity) 2 and 5 are inert in $K/\mathbb{Q}$.

(1) $\implies$ (2) for $n = 3$ by [AF67].

A Family of Number Fields

Definition

Let $p \nmid 2\ell$ be a rational prime. Define the number field $K(p)$ depending on p (and K) to be the composite of the fields $\{R(\mathfrak{p})\}_{\mathfrak{p}}$ as $\mathfrak{p}$ varies over all primes of K laying above p where $R(\mathfrak{p})$ is the unique quadratic subextension of $\mathrm{nR}^{\mathfrak{p}}/K$, the narrow ray class field over K of conductor $\mathfrak{p}$.

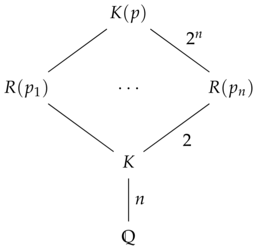

Figure 1: A field diagram depicting $K(p)$ in the case when p splits completely in $K/\mathbb{Q}$.

How can p factor in $K(p)/\mathbb{Q}$?

- p is always ramified in $K(p)/\mathbb{Q}$ with ramification index 2.
- If p splits completely in $K/\mathbb{Q}$ then there are 2 ways that p can factor in $K(p)/\mathbb{Q}$. Let $\mathfrak{p}$ denote a prime of K above p.

1. If $f_{R(\mathfrak{p}^\sigma)/K}(\mathfrak{p}) = 1$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ then $f_{K(p)/K}(\mathfrak{p}) = 1$.

   In other words, p "splits as completely as possible" in $K(p)/\mathbb{Q}$ (given the ramification).

2. If there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $f_{R(\mathfrak{p}^\sigma)/K}(\mathfrak{p}) = 2$ then $f_{K(p)/K}(\mathfrak{p}) = 2$.

With what density does p split as completely as possible?

$$S := \{\text{rational primes that split completely in } K/\mathbb{Q}\}$$
$$F := \{p \in S : f_{K(p)/K}(\mathfrak{p}) = 1\}$$

The density of $F \subseteq S$ restricted to S is defined as

$$d(F|S) := \lim_{N\to\infty} \frac{\{p \in F : p < N\}}{\{p \in S : p < N\}}$$

Conditional Theorem (5.5.3 in [McM18])

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

where m_K is a computable and bounded invariant of K.

Examples and Bounds

Recall $n = [K : \mathbb{Q}]$ and ℓ is the conductor.

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
$d(F\|S)$	$\frac{1}{4}$	$\frac{3}{64}$	$\frac{11}{512}$	$\frac{17}{32768}$	$\frac{33}{262144}$	$\frac{145}{16777216}$	$\frac{257}{134217728}$

$$\left(\frac{1}{2}\right)^{\frac{3n-1}{2}} \leq d(F|S) \leq \left(\frac{1}{2}\right)^{\frac{n+1}{2}}$$

A Conjecture on the Independence of Spin

$\mathscr{P}_K := \{\text{prime ideals of } \mathcal{O}_K\}$. For $\mathfrak{p} \in \mathscr{P}_K$, let $\alpha \in \mathcal{O}_K$ be a totally positive generator of $\mathfrak{p}^{h(K)}$. Define

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

$$\Lambda_\sigma := \{\mathfrak{p} \in \mathscr{P}_K : \text{spin}(\mathfrak{p}, \sigma) = 1\}.$$

Conjecture (A_n [McM18])

Let $\sigma, \tau \in \text{Gal}(K/\mathbb{Q})$ non-trivial such that $\sigma \neq \tau$ and $\sigma \neq \tau^{-1}$. Then

$$d(\Lambda_\sigma \cap \Lambda_\tau | \mathscr{P}_K) = d(\Lambda_\sigma | \mathscr{P}_K) d(\Lambda_\tau | \mathscr{P}_K).$$

This conjecture is within reach due to recent (not yet published) results of Djordjo Milovic and Peter Koymans.

A Conjecture on Character Sums

The following is a conjectural improvement to Burgess's result on short character sums coming from [FIMR13].

Conjecture (C_n [FIMR13])

Let χ be a non-principal real character mod q. Let $n \geq 3$, $Q \geq 3$, $N \leq Q^{\frac{1}{n}}$, and $q \leq Q$. Then

$$\sum_{M<n<M+N} \chi(n) << Q^{\frac{1-\delta}{n}+\epsilon},$$

with some $\delta = \delta(n) > 0$ and any $\epsilon > 0$, the implied constant depending only on ϵ and δ.

Remark

Conjecture C_n is true for $n = 3$ by Burgess's bound.

Computational Aspect

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

- m_K is defined as the number of Gal$(K/\mathbb{Q})$-orbits of $\mathbf{M}_4$ of size-n such that $(\alpha, \alpha^\sigma)_2 = 1$ for all $\sigma \neq 1 \in$ Gal$(K/\mathbb{Q})$ where α is a representative in $\mathcal{O}_K$.
- Currently, finding m_K involves a computation depending on the number field K, though I am working towards a formula for m_K depending only on $n = [K : \mathbb{Q}]$.
- In particular, with an added assumption on K, I am close to a proof that $m_K = 1$ whenever $n = 3$.

Ideas Behind the Proof

$$R := \{\mathfrak{p} \in S : \text{spin}(\mathfrak{p}, \sigma) = \text{spin}(\mathfrak{p}, \sigma^{-1})\}$$

$$F \subseteq R \subseteq S$$

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

Using some class field theory and Dirichlet/Chebotarev's Density Theorem, we arrive at Theorem 7.2 of [McMng], which gives

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

If Conjectures C_n and A_n are true, then by the main results of [FIMR13],

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

Bibliography

J. V. Armitage and A. Fröhlich, *Classnumbers and unit signatures*, Mathematika **14** (1967), 94–98. MR 0214566

J. B. Friedlander, H. Iwaniec, B. Mazur, and K. Rubin, *The spin of prime ideals*, Invent. Math. **193** (2013), no. 3, 697–749. MR 3091978

Christine McMeekin, *A density of ramified primes*, ProQuest LLC, Ann Arbor, MI, 2018, Thesis (Ph.D.)–Cornell University, (pending publication).

Christine McMeekin, *On the asymptotics of prime spin relations*, (publication pending), arXiv:1807.00892.