On The Distribution of Splitting Behavior in Number Fields Depending on p

Christine McMeekin

Cornell University

August 13, 2016

Outline

Introduction (1/3)

- Classically one might consider fixing a number field K and asking how various primes p split in K.
  - Dirichlet's Theorem
  - Chebotarev's Theorem
- Others have worked on fixing p and varying K with fixed Galois group.
  - Bhargava, Cohen, Datskovsky, Davenport, Heilbronn, Taylor, Wood, Wright, and more.
- We will construct a field K_p depending on p and K and for fixed K we will give distribution conjectures and results for how p splits in K_p as p varies. In this talk we will focus on the case where $[K : \mathbb{Q}] = 3$.

Introduction (2/3)

- When K satisfies certain conditions, there will be a unique quadratic extension of K ramified only at a particular prime $\mathfrak{p}$ of K and the infinite places.

Introduction (2/3)

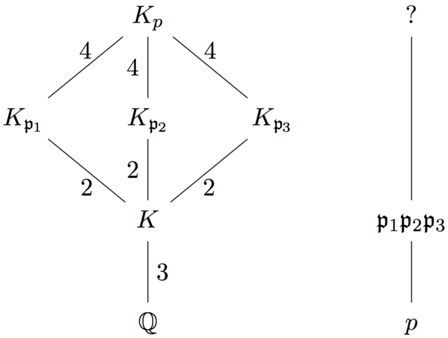
- When K satisfies certain conditions, there will be a unique quadratic extension of K ramified only at a particular prime $\mathfrak{p}$ of K and the infinite places.
- We denote this extension $K_{\mathfrak{p}}$.

Introduction (2/3)

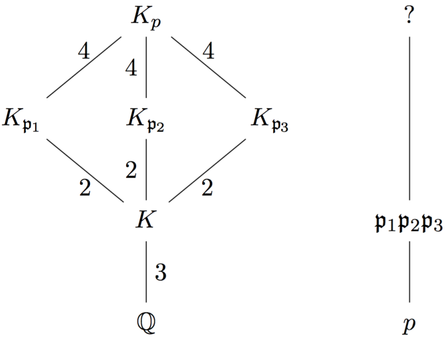
- When K satisfies certain conditions, there will be a unique quadratic extension of K ramified only at a particular prime $\mathfrak{p}$ of K and the infinite places.
- We denote this extension $K_{\mathfrak{p}}$.
- We let p be a rational prime which splits completely in K; $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

Introduction (2/3)

- When K satisfies certain conditions, there will be a unique quadratic extension of K ramified only at a particular prime $\mathfrak{p}$ of K and the infinite places.
- We denote this extension $K_{\mathfrak{p}}$.
- We let p be a rational prime which splits completely in K; $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.
- We let K_p be the composite of all three $K_{\mathfrak{p}_i}$.



Introduction (3/3)



- We will see that there are only two ways p can split in K_p. Our goal is to determine how often p splits one way verses the other.

Construction of K_p (1/4)

Notation:

- $h(K)$ denotes the class number of K.
- U denotes the units of the ring of integers of K.
- U_T denotes the totally positive units.
- $\mathfrak{m}_\infty$ denotes the product of all infinite places in K.

Construction of K_p (1/4)

Notation:

- $h(K)$ denotes the class number of K.
- U denotes the units of the ring of integers of K.
- U_T denotes the totally positive units.
- $\mathfrak{m}_\infty$ denotes the product of all infinite places in K.

Theorem (M)

Let K be a number field such that

- *K is totally real*
- *$h(K)$ is odd*
- *$U_T = U^2$*

Let $\mathfrak{p}$ be a prime in K which is prime to 2. Then the ray class field of conductor $\mathfrak{p}\mathfrak{m}_\infty$ has a unique quadratic subextension, which we will denote $K_\mathfrak{p}$.

Construction of K_p (2/4)

Many number fields satisfy the necessary conditions. (Later we will also need $K/\mathbb{Q}$ to be Galois, cyclic, and cubic).

- Armitage and Frohlich have a theorem which gives an easy condition implying $U_T = U^2$.
- Example: If K is the unique cubic subextension of the l^{th} cyclotomic field for $l \equiv 1 \mod 3$ prime, then all we need is $h(K)$ to be odd, (which happens often) and we will have met all the conditions.

Construction of K_p (3/4)

Let K be a number field such that

Construction of K_p (3/4)

Let K be a number field such that

- K is totally real
- $h(K)$ is odd
- $U_T = U^2$
- $K/\mathbb{Q}$ is Galois, cyclic, and cubic

Construction of K_p (3/4)

Let K be a number field such that

- K is totally real
- $h(K)$ is odd
- $U_T = U^2$
- $K/\mathbb{Q}$ is Galois, cyclic, and cubic

Let $p \neq 2$ be a rational prime which splits completely in K; $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

Construction of K_p (3/4)

Let K be a number field such that

- K is totally real
- $h(K)$ is odd
- $U_T = U^2$
- $K/\mathbb{Q}$ is Galois, cyclic, and cubic

Let $p \neq 2$ be a rational prime which splits completely in K; $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

- Define K_p to be the composite of all three $K_{\mathfrak{p}_i}$. Recall that $K_{\mathfrak{p}_i}$ is the unique quadratic subextension of the ray class field over K of conductor $\mathfrak{p}_i\mathfrak{m}_\infty$.

Construction of K_p (3/4)

Let K be a number field such that

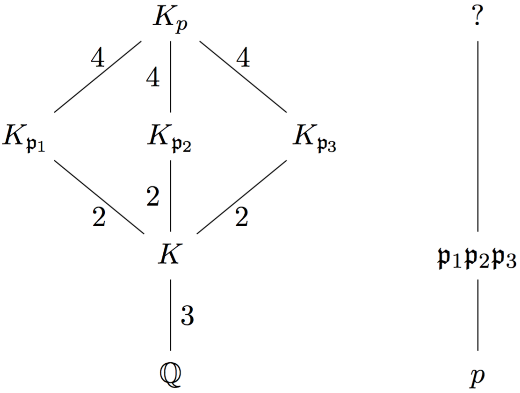
- K is totally real
- $h(K)$ is odd
- $U_T = U^2$
- $K/\mathbb{Q}$ is Galois, cyclic, and cubic

Let $p \neq 2$ be a rational prime which splits completely in K; $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

- Define K_p to be the composite of all three $K_{\mathfrak{p}_i}$. Recall that $K_{\mathfrak{p}_i}$ is the unique quadratic subextension of the ray class field over K of conductor $\mathfrak{p}_i\mathfrak{m}_\infty$.
- In other words, $\mathfrak{p}_i$ and the infinite places are the only places which ramify in the quadratic extension $K_{\mathfrak{p}_i}/K$.

Construction of K_p (4/4)

We have the following diagram.



We ask how p splits in K_p.

How can p split in K_p? (1/2)

Note that $K_p/\mathbb{Q}$ is Galois. Also note that in the case of cubic K, $[K_p : \mathbb{Q}] = 24$.

How can p split in K_p? (1/2)

Note that $K_p/\mathbb{Q}$ is Galois. Also note that in the case of cubic K, $[K_p : \mathbb{Q}] = 24$.

- We know $e = 2$ (e=ramification index of p in $K_p/\mathbb{Q}$)

How can p split in K_p? (1/2)

Note that $K_p/\mathbb{Q}$ is Galois. Also note that in the case of cubic K, $[K_p : \mathbb{Q}] = 24$.

- We know $e = 2$ (e=ramification index of p in $K_p/\mathbb{Q}$)
- We know $3|g$ (g=number of distinct primes above p in $K_p/\mathbb{Q}$)

How can p split in K_p? (1/2)

Note that $K_p/\mathbb{Q}$ is Galois. Also note that in the case of cubic K, $[K_p : \mathbb{Q}] = 24$.

- We know $e = 2$ (e=ramification index of p in $K_p/\mathbb{Q}$)
- We know $3|g$ (g=number of distinct primes above p in $K_p/\mathbb{Q}$)
- So f can only be 1, 2, or 4. (f=inertia degree of p in $K_p/\mathbb{Q}$)

How can p split in K_p? (1/2)

Note that $K_p/\mathbb{Q}$ is Galois. Also note that in the case of cubic K, $[K_p : \mathbb{Q}] = 24$.

- We know $e = 2$ (e=ramification index of p in $K_p/\mathbb{Q}$)
- We know $3|g$ (g=number of distinct primes above p in $K_p/\mathbb{Q}$)
- So f can only be 1, 2, or 4. (f=inertia degree of p in $K_p/\mathbb{Q}$) However, f can not be 4 because residue field extensions are cyclic and embed into the Galois group but K_p/K has no cyclic subextension of degree 4.

How can p split in K_p? (1/2)

Note that $K_p/\mathbb{Q}$ is Galois. Also note that in the case of cubic K, $[K_p : \mathbb{Q}] = 24$.

- We know $e = 2$ (e=ramification index of p in $K_p/\mathbb{Q}$)
- We know $3|g$ (g=number of distinct primes above p in $K_p/\mathbb{Q}$)
- So f can only be 1, 2, or 4. (f=inertia degree of p in $K_p/\mathbb{Q}$) However, f can not be 4 because residue field extensions are cyclic and embed into the Galois group but K_p/K has no cyclic subextension of degree 4.

Therefore there are only two ways p can split in $K_p/\mathbb{Q}$; $f = 1$ or $f = 2$.

How can p split in K_p? (2/2)

Let $f(\mathfrak{p}_i)_j$ denote the inertia degree of $\mathfrak{p}_i$ in $K_{\mathfrak{p}_j}/K$.

Remark

Due to the action of Gal$(K/\mathbb{Q})$ on $\{K_{\mathfrak{p}_1}, K_{\mathfrak{p}_2}, K_{\mathfrak{p}_3}\}$, we have $f(\mathfrak{p}_1)_2 = f(\mathfrak{p}_2)_3 = f(\mathfrak{p}_3)_1$ and $f(\mathfrak{p}_2)_1 = f(\mathfrak{p}_1)_3 = f(\mathfrak{p}_3)_2$

How can p split in K_p? (2/2)

Let $f(\mathfrak{p}_i)_j$ denote the inertia degree of $\mathfrak{p}_i$ in $K_{\mathfrak{p}_j}/K$.

Remark

Due to the action of $Gal(K/\mathbb{Q})$ *on* $\{K_{\mathfrak{p}_1}, K_{\mathfrak{p}_2}, K_{\mathfrak{p}_3}\}$, *we have* $f(\mathfrak{p}_1)_2 = f(\mathfrak{p}_2)_3 = f(\mathfrak{p}_3)_1$ *and* $f(\mathfrak{p}_2)_1 = f(\mathfrak{p}_1)_3 = f(\mathfrak{p}_3)_2$

- Therefore, the way p splits in K_p is completely determined by knowing only how $\mathfrak{p}_1$ splits in $K_{\mathfrak{p}_2}$ and how $\mathfrak{p}_2$ splits in $K_{\mathfrak{p}_1}$.

How can p split in K_p? (2/2)

Let $f(\mathfrak{p}_i)_j$ denote the inertia degree of $\mathfrak{p}_i$ in $K_{\mathfrak{p}_j}/K$.

Remark

Due to the action of Gal$(K/\mathbb{Q})$ on $\{K_{\mathfrak{p}_1}, K_{\mathfrak{p}_2}, K_{\mathfrak{p}_3}\}$, we have $f(\mathfrak{p}_1)_2 = f(\mathfrak{p}_2)_3 = f(\mathfrak{p}_3)_1$ and $f(\mathfrak{p}_2)_1 = f(\mathfrak{p}_1)_3 = f(\mathfrak{p}_3)_2$

- Therefore, the way p splits in K_p is completely determined by knowing only how $\mathfrak{p}_1$ splits in $K_{\mathfrak{p}_2}$ and how $\mathfrak{p}_2$ splits in $K_{\mathfrak{p}_1}$.
- If one or both of $f(\mathfrak{p}_1)_2$ or $f(\mathfrak{p}_2)_1$ is 2, then $f = 2$ in $K_p/\mathbb{Q}$. Otherwise $f = 1$.

Spin (1/3)

Definition

Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Given an odd principal ideal $\mathfrak{a}$ we define the spin of $\mathfrak{a}$ to be

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

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

Spin (1/3)

Definition

Let $\sigma \in \text{Gal}(K/\mathbb{Q})$. Given an odd principal ideal $\mathfrak{a}$ we define the spin of $\mathfrak{a}$ to be

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

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

- Friedlander, Iwaniec, Mazur, and Rubin have results on the distribution of spin. We will relate spin to how p splits in K_p to obtain distribution results there.

Spin (2/3)

Let α_i denote a totally positive generator for $\mathfrak{p}_i$.

Theorem (M)

$\left(\frac{\alpha_i}{\mathfrak{p}_j}\right) = 1$ if and only if $\mathfrak{p}_i$ splits in $K_{\mathfrak{p}_j}$.

Spin (2/3)

Let α_i denote a totally positive generator for $\mathfrak{p}_i$.

Theorem (M)

$\left(\frac{\alpha_i}{\mathfrak{p}_j}\right) = 1$ *if and only if* $\mathfrak{p}_i$ *splits in* $K_{\mathfrak{p}_j}$.

Idea of proof:

Spin (2/3)

Let α_i denote a totally positive generator for $\mathfrak{p}_i$.

Theorem (M)

$\left(\frac{\alpha_i}{\mathfrak{p}_j}\right) = 1$ *if and only if* $\mathfrak{p}_i$ *splits in* $K_{\mathfrak{p}_j}$.

Idea of proof:

Lemma

$K_{\mathfrak{p}_i} = K(\sqrt{u_i \alpha_i})$ *for some unit* u_i *well-defined modulo squares.*

Spin (2/3)

Let α_i denote a totally positive generator for $\mathfrak{p}_i$.

Theorem (M)

$\left(\frac{\alpha_i}{\mathfrak{p}_j}\right) = 1$ *if and only if* $\mathfrak{p}_i$ *splits in* $K_{\mathfrak{p}_j}$.

Idea of proof:

Lemma

$K_{\mathfrak{p}_i} = K(\sqrt{u_i \alpha_i})$ *for some unit* u_i *well-defined modulo squares.*

Lemma

$$\left(\frac{u_j \alpha_j}{\mathfrak{p}_i}\right) = \left(\frac{\alpha_i}{\mathfrak{p}_j}\right)$$

Spin (2/3)

Let α_i denote a totally positive generator for $\mathfrak{p}_i$.

Theorem (M)

$\left(\frac{\alpha_i}{\mathfrak{p}_j}\right) = 1$ if and only if $\mathfrak{p}_i$ splits in $K_{\mathfrak{p}_j}$.

Idea of proof:

Lemma

$K_{\mathfrak{p}_i} = K(\sqrt{u_i \alpha_i})$ for some unit u_i well-defined modulo squares.

Lemma

$$\left(\frac{u_j \alpha_j}{\mathfrak{p}_i}\right) = \left(\frac{\alpha_i}{\mathfrak{p}_j}\right)$$

Let $\mathfrak{b}_i$ denote a prime in $K_{\mathfrak{p}_j}$ above $\mathfrak{p}_i$. The injective homomorphism

$$\mathcal{O}_K/\mathfrak{p}_i \to \mathcal{O}_{K_{\mathfrak{p}_j}}/\mathfrak{b}_i$$

is surjective iff $f(\mathfrak{p}_i)_j = 1$ iff $\left(\frac{u_j \alpha_j}{\mathfrak{p}_i}\right) = 1$.

Spin (3/3)

- Let σ be the generator of $\mathrm{Gal}(K/\mathbb{Q})$ mapping the indices of $\mathfrak{p}_i$ according the the permutation (123).
- Let $f(\mathfrak{p}_i)_j$ denote the inertia degree of $\mathfrak{p}_i$ in $K_{\mathfrak{p}_j}/K$. (This can only be 1 or 2.)

Corollary

$$spin(\mathfrak{p}_1, \sigma) = -1 \iff f(\mathfrak{p}_1)_2 = 2$$

$$spin(\mathfrak{p}_1, \sigma^2) = -1 \iff f(\mathfrak{p}_2)_1 = 2$$

FIMR results (1/2)

Recall K satisfies the following:

- K is totally real
- $h(K)$ is odd
- $U_T = U^2$
- K is Galois, cyclic, and cubic.

FIMR results (1/2)

Recall K satisfies the following:

- K is totally real
- $h(K)$ is odd
- $U_T = U^2$
- K is Galois, cyclic, and cubic.

Theorem (FIMR)

Letting $\mathfrak{p}$ run over odd prime principal ideals in K,

$$\left| \sum_{N(\mathfrak{p})<x} spin(\mathfrak{p}, \sigma) \right| << x^{1-\frac{1}{10656}+\epsilon}$$

FIMR results (1/2)

Recall K satisfies the following:

- K is totally real
- $h(K)$ is odd
- $U_T = U^2$
- K is Galois, cyclic, and cubic.

Theorem (FIMR)

Letting $\mathfrak{p}$ run over odd prime principal ideals in K,

$$\left| \sum_{N(\mathfrak{p})<x} spin(\mathfrak{p}, \sigma) \right| << x^{1-\frac{1}{10656}+\epsilon}$$

Idea: spin=1 half the time and spin=-1 half the time

FIMR results (2/2)

Theorem (Main Theorem- M)

$f = 2$ for p in $K_p/\mathbb{Q}$ at least 50% of the time

FIMR results (2/2)

Theorem (Main Theorem- M)

$f = 2$ for p in $K_p/\mathbb{Q}$ at least 50% of the time

- Due to FIMR results, we know $f(\mathfrak{p}_1)_2 = 2$ half the time *and* $f(\mathfrak{p}_2)_1 = 2$ half the time.

FIMR results (2/2)

Theorem (Main Theorem- M)

$f = 2$ for p in $K_p/\mathbb{Q}$ at least 50% of the time

- Due to FIMR results, we know $f(\mathfrak{p}_1)_2 = 2$ half the time *and* $f(\mathfrak{p}_2)_1 = 2$ half the time.
- We do not know these events are independent, but if we knew that the following conjecture would be true.

Conjecture (M)

The probability that $f = 1$ for p in $K_p/\mathbb{Q}$ is $\frac{1}{4}$ and the probability that $f = 2$ is $\frac{3}{4}$

Data (1/1)

Let p run over the first 10,000 primes which split completely in K excluding 2. The first column l defines the number field K, which is the unique cubic subextension of the l^{th} cyclotomic field for prime $l \equiv 1 \mod 3$. The second column gives the number of times $f = 1$ in $K_p/\mathbb{Q}$.

l	$f = 1$
7	2480
13	2455
19	2511
31	2434
37	2559
43	2502
61	2503
67	2516
73	2472
79	2495
97	2485

Further Work (1/1)

- Show $f(\mathfrak{p}_1)_2$ and $f(\mathfrak{p}_2)_1$ are independent to prove conjecture.

Further Work (1/1)

- Show $f(\mathfrak{p}_1)_2$ and $f(\mathfrak{p}_2)_1$ are independent to prove conjecture.
- A generalization of FIMR's Theorem to the case when $[K : \mathbb{Q}] > 3$ (and thus a generalization of splitting results for p in K_p) relies on a conjectural improvement on Burgess's Theorem on short character sums.

Further Work (1/1)

- Show $f(\mathfrak{p}_1)_2$ and $f(\mathfrak{p}_2)_1$ are independent to prove conjecture.
- A generalization of FIMR's Theorem to the case when $[K : \mathbb{Q}] > 3$ (and thus a generalization of splitting results for p in K_p) relies on a conjectural improvement on Burgess's Theorem on short character sums.
- If a similar result to FIMR worked for imaginary quadratic fields, there would be interesting applications to elliptic curves.