Asymptotics For Number Fields And Class Groups

Project Group: Expected expectations

Melanie Matchett Wood

Assisted by Robert Harron

Aleksander Beloi

Ziyue Guo

Catherine Hsu

Silas Johnson

Cihan Karahulut

Michiel Kusters

Jonah Leshin

Jingbo Liu

Patrick Meisner

James Weigandt

Chao Li

Evan Dummit

Rachel Davis

Distributions of Class Groups

Quadratic fields

- conditions at infinity (Real vs. Imag.) has a big effect on the class group.
- MB-heuristics imply non-arch local cond. have no effect.

Goal: Investigate this in further cases (higher degree) (more conditions)

Cubic fields (K cubic field)

How to count $\#Sur(Cl(K), \mathbb{Z}/2\mathbb{Z})$?

Do local conditions affect this?

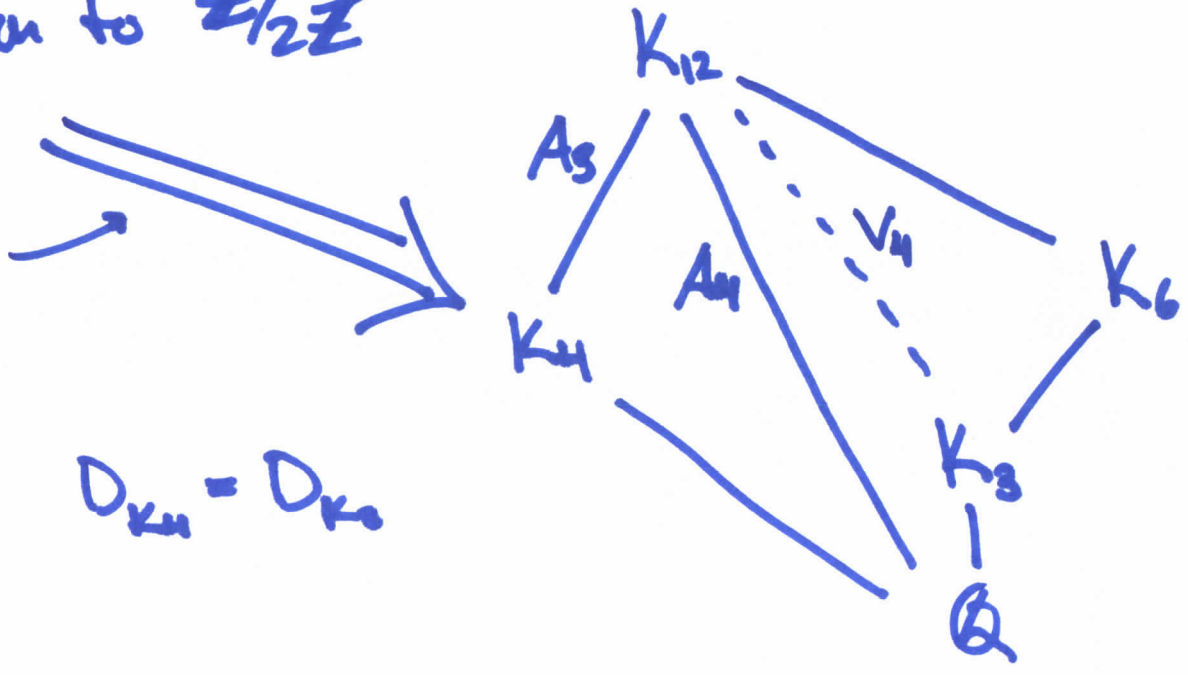
Condition at ∞: K_3 cyclic cubic (totally real)

+

Surjection to $\mathbb{Z}/2\mathbb{Z}$

Heilbronn

s.t. $D_{K_{12}} = D_{K_6}$



Decomposition Group	Inertia Group	Splitting Type in K_3	Splitting Type in K_4
1	1	$(1,1,1)$	$(1,1,1,1)$
$\langle(123)\rangle$	1	(3)	$(1,3)$
* $\langle(123)\rangle$	(123)	(1^3)	$(1,1^3)$
$\langle(12)(34)\rangle$	1	$(1,1,1)$	$(2,2)$
* $\langle(12)(34)\rangle$	$(12)(34)$	$(1,1,1)$	$(1^2,1^2)$
$W_4 = V_4$	$(12)(34)$	$(1,1,1)$	(2^2)

$$\#\left\{\mathrm{Gal}(\mathrm{Cl}(K_3), \mathbb{Z}/2\mathbb{Z}) : K_3 \text{ cyclic cubic}, \text{ totally split at } 7 \right\}$$
$$|D_{K_3}| < X$$

??

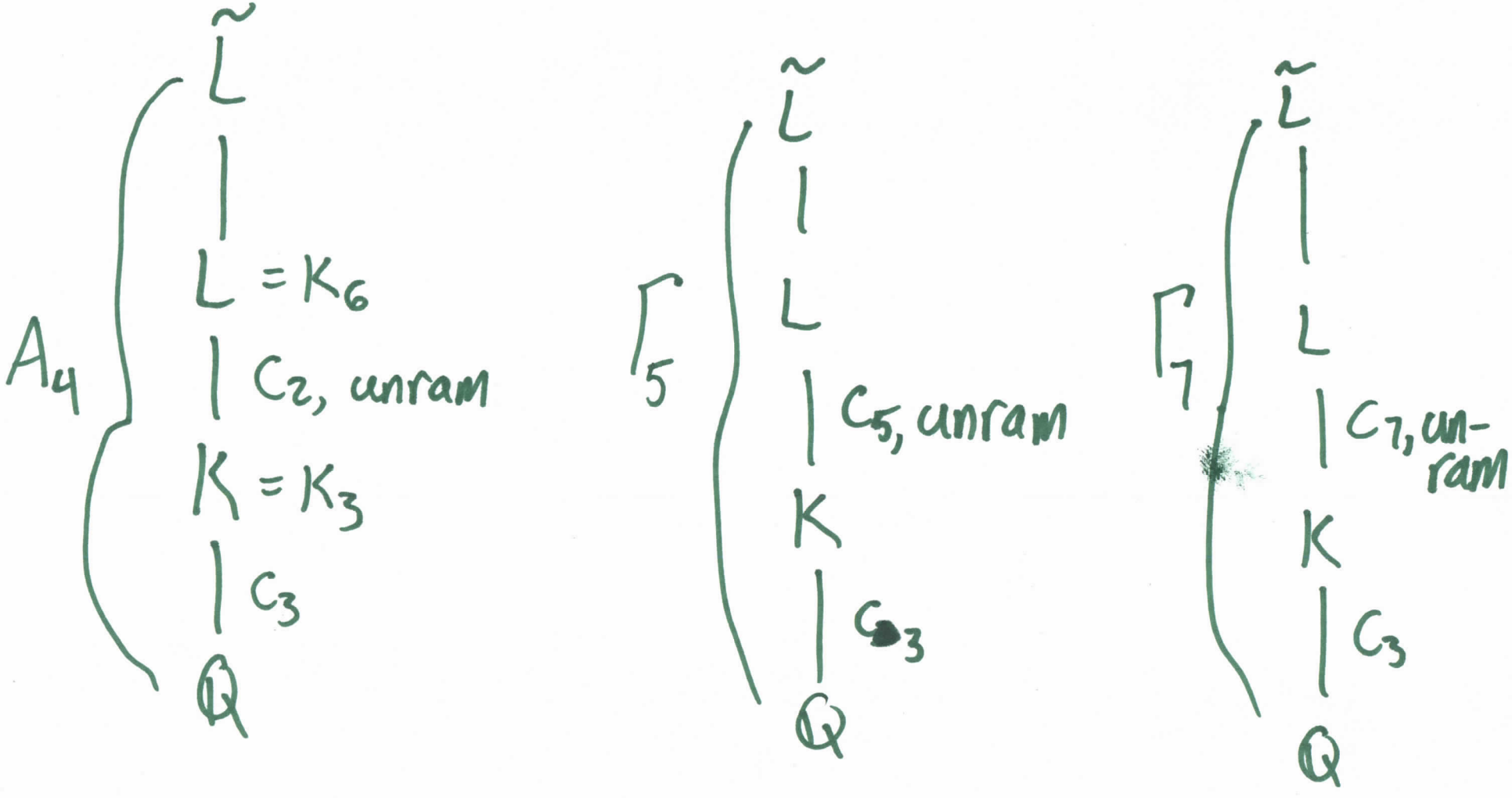
$$\#\left\{ |D_{K_4}| < X : K_4 \ A_4\text{-quartic}, \text{ totally split at } 7 \text{ or } (7) = P_1 P_2 \right\}$$
$$+(\text{Extra conditions})$$

Bhargava has results on counting S_4-quartics

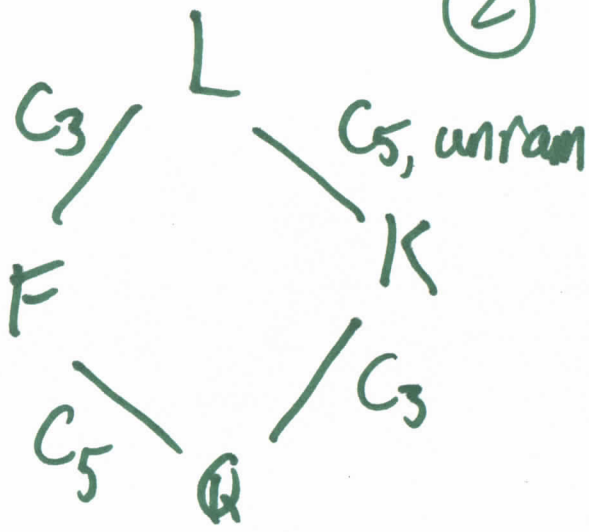
. . . but we dont know how to count A_4-quartics.

We can still compute local factors and make predictions using MB-heuristics, in this and more difficult cases.

Possible Galois Groups



$\Gamma_5 \cong (C_5)^K \rtimes C_3$; $\underline{K \neq 1}$:



$\underline{K \neq 3}$: $C_3 = \langle \alpha \rangle$. α acting on $(C_5)^3$ must have 1 as an eigenvalue.

$\Rightarrow \Gamma_5 \cong *(C_5 \times C_5) \rtimes (C_5 \times C_3)$

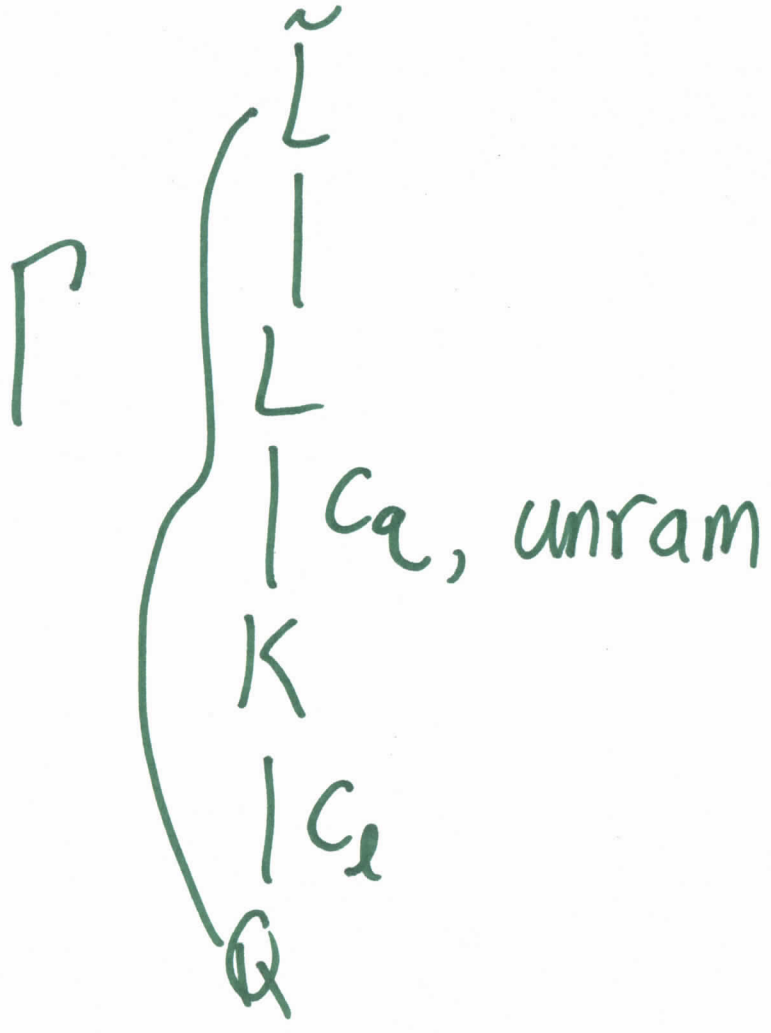
$\Rightarrow$ Unram extension of $\mathbb{Q}$. #

$\Gamma_7 \cong (C_7)^k \rtimes C_3$; $k = 1, 2, \text{ or } 3$.

Although: • α acting on $(C_7)^k$ cannot have 1 as an eigenvalue.

• If $k \geq 2$, all eigenvalues of α cannot be the same.

More generally: $\Gamma \cong (C_q)^K \rtimes C_\ell$



Notation:

- $C_\ell = \langle \alpha \rangle$, α acts on $(C_q)^K$ by φ_α.
- $\forall \alpha \in \Gamma$, $v \in (C_q)^K$

Proposition

1) φ_a cannot have any eigenvalues $= 1$

2) If $\kappa \geq 2$, all eigenvalues of φ_a cannot be the same.

3) $q^\kappa \equiv 1 \pmod{\ell}$

And, 1) implies:

4) There are $\ell - 1$ conjugacy classes of elements of order ℓ.

proof of 4)

a) Total # elts order ℓ is $q^k(\ell-1)$:

$$(V_\alpha)^\ell = (v + \varphi_\alpha(v) + \cdots + \varphi_\alpha^{\ell-1}(v)) \cdot \alpha^\ell$$

$$= (I + \varphi_\alpha + \cdots + \varphi_\alpha^{\ell-1})(v)$$

$= 0$ b/c 1 not an eigenvalue of φ_α.

b) # elts in each C. class of order ℓ element is $(q^k \cdot \ell)/\ell = q^k$.

c) Therefore, # conjugacy classes of elts of order ℓ is

$$\frac{q^k(\ell-1)}{q^k} = \ell - 1. \quad //$$

Local Factors

$\tilde{L}$
$|$
L
$\text{nr} \,|\, C_q$
K
$|\, C_\ell$
$\mathbb{Q}$

$$\Gamma = \mathrm{Gal}(\tilde{L}/\mathbb{Q}) = \underset{\substack{\uparrow \\ A}}{C_q^k} \rtimes C_\ell$$

Goal: Determine the local factors in Malle-Bhargava for counting these.

$$\mathbb{E}(\#\mathrm{Surj}(\mathrm{Cl}(K) \to C_q)) = ?$$

Local factor at p: $(p \neq \ell)$

$$\sum_{\substack{[y] \in \Gamma \\ \text{with } [y] = [y^p]}} (\operatorname{disc} y)^{-s}$$

Also restrict to $y \notin A$ (else L/K ram.)

$\iff$ $y = v\alpha$ for $v \in A$, $\alpha \in C_\ell$, $\alpha \neq id$

$\iff$ $\operatorname{ord}(y) = \ell$

(or $y = 1$)

Facts:

- Γ has $(\ell-1)$ conjugacy classes of elements of order ℓ.
- If y has order ℓ, its centralizer is $\langle y \rangle$.
- $[y] = \{v'\alpha : v' \in A\}$ $(y = v\alpha)$
- $y^p = v'\alpha^p$ for some $v' \in A$.

Thus $[y]=[y^p] \iff \alpha = \alpha^p$

$\iff p \equiv 1 \mod \ell$

Local factor is:

- 1 if $p \not\equiv 1 \mod \ell$
- $1 + (\ell-1)p^{-(\ell-1)s}$ if $p \equiv 1 \mod \ell$
- Hard if $p = \ell$.

Same as local factor for counting C_ℓ fields!

Local restrictions?

Ex: Require p to split completely in K.

Requires $K/\mathbb{Q}$ unram. at p,
and $\mathrm{Frob}_p \in A$. (For C_ℓ $\mathrm{Frob}_p = 1$.)

$$\text{Local factor} = \frac{1}{|\Gamma|} \sum_{\rho : G_{\mathbb{Q}_p} \to \Gamma} (\text{disc}\, \rho)^{-s}$$

$$= \frac{1}{|\Gamma|} (\#\, \text{Frob})$$

For $\Gamma = A \times C_\ell$, $\quad \frac{1}{q^k \cdot \ell} \cdot q^k = \frac{1}{\ell}$

For C_ℓ, $\quad \frac{1}{\ell} \cdot 1 = \frac{1}{\ell}$

Even if we have to sum up over several possible Γ, this $\frac{1}{2}$ is independent of Γ, so it doesn't matter.

Ramified local conditions?

Ex: Let $\mathcal{K}/\mathbb{Q}_p$ $(p \equiv 1 \bmod \ell)$ be a totally ramified C_ℓ extn.

Require $K_p = \mathcal{K}$.

$\rho : G_{\mathbb{Q}_p} \to \Gamma$ is given by

x, y with $xyx^{-1} = y^p = y$.

$\Longrightarrow x \in \langle y \rangle$

$\Longrightarrow \operatorname{im} \rho \simeq C_\ell$

$\Longrightarrow \rho : G_{\mathbb{Q}_p} \xrightarrow{\rho_1} C_\ell \xrightarrow{\rho_2} \Gamma$

ρ_1 determines K_p.

ρ_1, ρ_2 are independent,

so all K occur equally often.

Jones-Roberts: There are ℓ of them.

$$\text{Local factor} = \frac{\ell - 1}{\ell} p^{-(\ell-1)s}$$

Same for C_ℓ.

Moral:

Consider $\mathbb{E}\left(\#\mathrm{Surj}\left(Cl(K) \to C_\ell\right)\right)$

as K ranges through

C_ℓ-extensions of $\mathbb{Q}$.

Tame, non-arch

The Malle-Bhargava $\Rightarrow$ <u>any</u> local condition on K does not affect this.

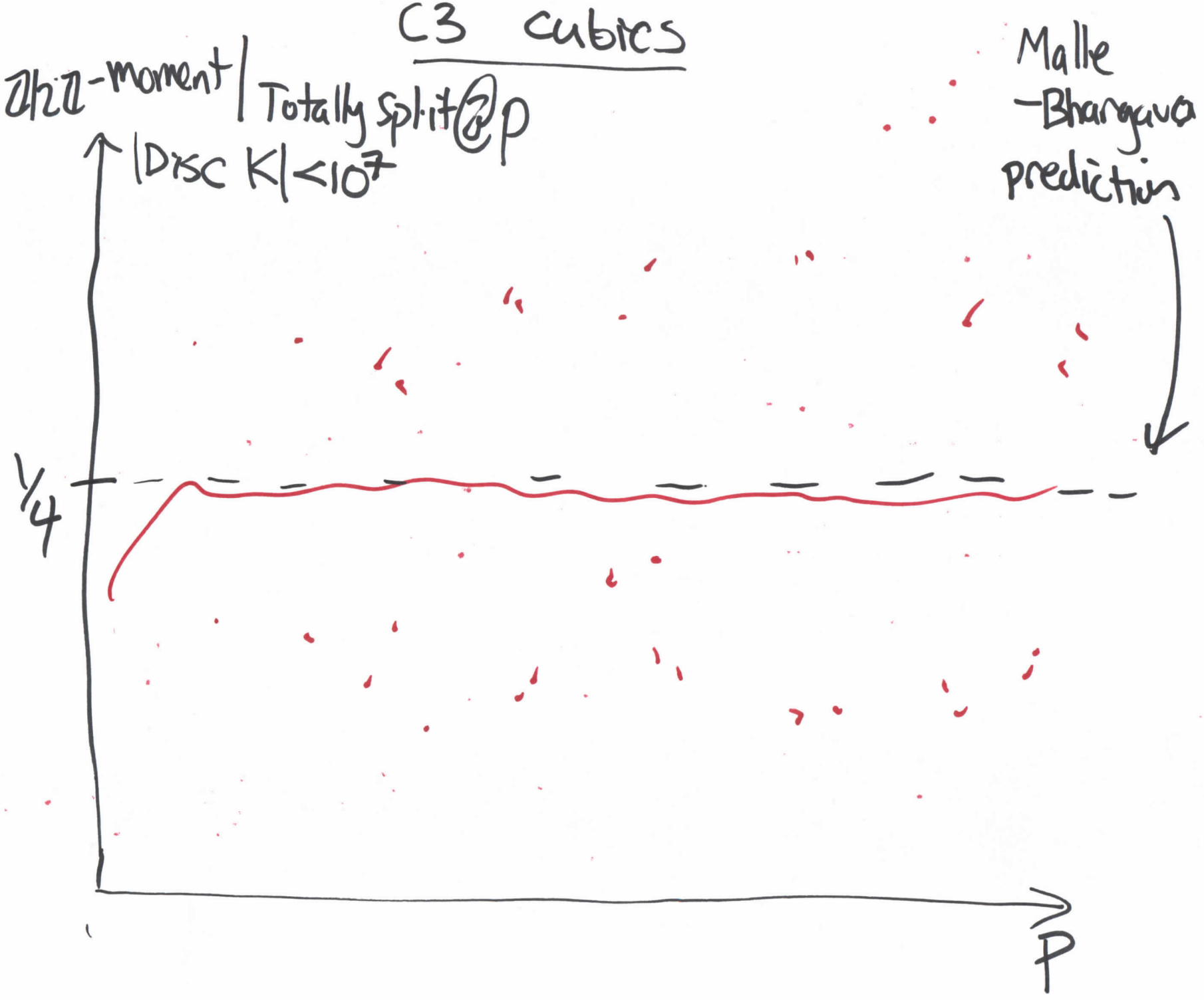
Let $D(G,X) = \left\{ \begin{array}{c} \text{cubic fields} \\ K \end{array} \;\middle|\; \begin{array}{l} \mathrm{Gal}(K) \simeq G \\ |\mathrm{Disc}\, K| < X \end{array} \right\}$

Using data for cubics with $|\mathrm{Disc}\, K| < 10^7$, we computed

$$\frac{1}{\#D(C_3, 10^7)} \sum_{K \in D(C_3, 10^7)} \frac{\#\mathrm{Sur}(\mathrm{Cl}(\mathcal{O}_K), \mathbb{Z}/2\mathbb{Z})}{\#\mathrm{Cl}(\mathcal{O}_K)[2] - 1} \approx 0.26$$

and for primes $p < 1000$

$$\frac{1}{\#D(C_3, 10^7; p \text{ totally split})} \sum_{\substack{K \in D(C_3, 10^7), \\ p \text{ totally split}}} \#\mathrm{Sur}(\mathrm{Cl}(\mathcal{O}_K), \mathbb{Z}/2\mathbb{Z})$$

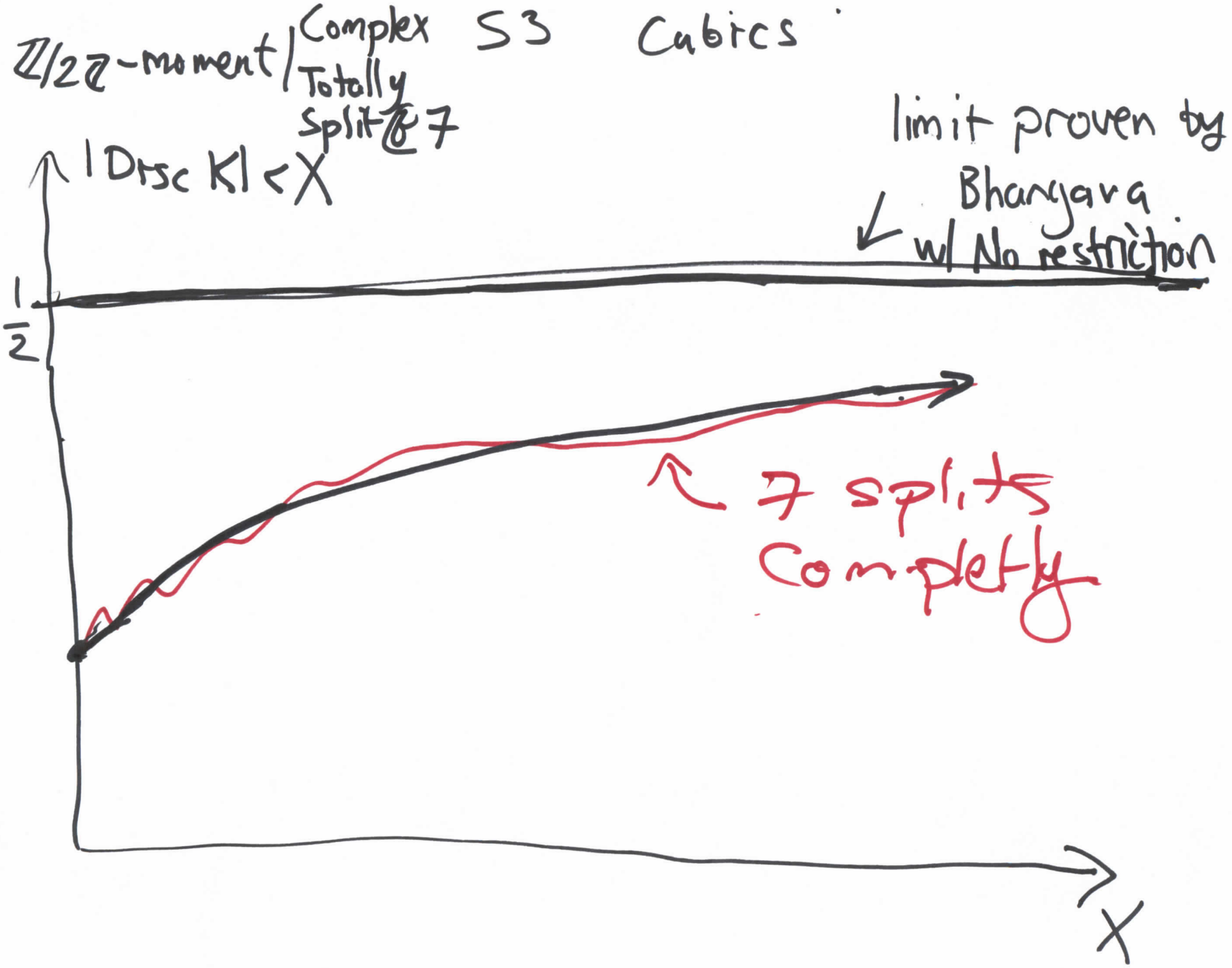

C3 cubics
2nd-moment | Totally split@p
|Disc K|<10^7
Malle
-Bhargava
prediction
1/4
p

For various $X < 10^7$ we computed and compared.

$$\frac{\sum_{\text{complex } K/\mathbb{Q}\ S_3\text{-cubic } |\mathrm{Disc}\, K| < X} \#\mathrm{Sur}(\mathrm{Cl}(\mathcal{O}_K), \mathbb{Z}/2\mathbb{Z})}{\sum_{K/\mathbb{Q}\ S_3\text{-cubic, complex } |\mathrm{Disc}\, K| < X} 1} \to \frac{1}{2}$$

AND

$$\frac{\sum_{\text{complex } K/\mathbb{Q}\ S_3\text{-cubic } |\mathrm{Disc}\, K| < X,\ 7 \text{ totally split in } \mathcal{O}_K} \#\mathrm{Sur}(\mathrm{Cl}(\mathcal{O}_K), \mathbb{Z}/2\mathbb{Z})}{\sum_{\text{same}} 1}$$


1/2-moment
Complex
Totally
Split@7
S3
Cubics
|Disc K| < X
limit proven by
Bhargava
w/ No restriction
1/2
7 splits
Completly
X

Non-Cyclic Cubic Fields:

(1) Establish the relationship between unramified quadratic extensions K_6 of cubic fields K_3 and quartic fields K_4

(2) When K_3 is split completely at some rational prime l into $l_1 l_2 l_3$, determine what the condition on K_4 is for Frob_{l_1} to be trivial in the Galois group $\mathrm{Gal}(K_6/K_3)$ of the unramified extn.

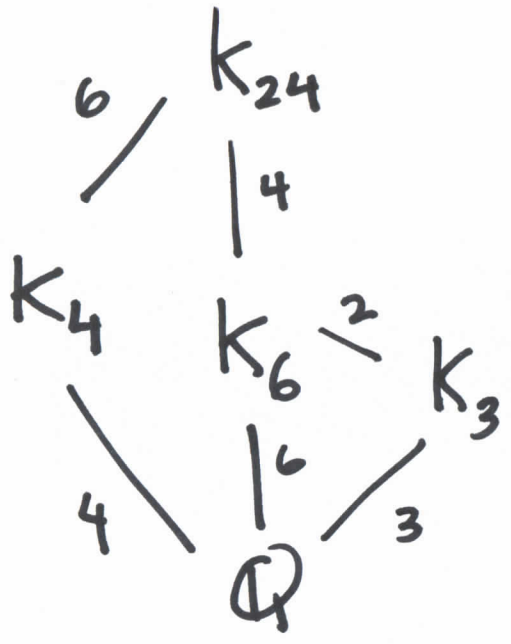
(3) Combine (1) & (2) in order to translate the following global question:

Q: How frequently are l_1, l_2, l_3 all trivial in order two quotients of the class group of K_3? (The other option is l_1 trivial and l_2, l_3 nontrivial.)

→ case 1

→ case 2

(4) Apply a theorem of Bhargava to answer the question above, namely count quartic fields with certain local conditions.



$\text{Gal}(K_{24}/\mathbb{Q}) \cong S_4$

$\text{Gal}(K_{24}/K_6) \cong V_4$

$\text{Gal}(K_{24}/K_3) \cong D_4$

$\text{Gal}(K_{24}/K_4) \cong S_3$

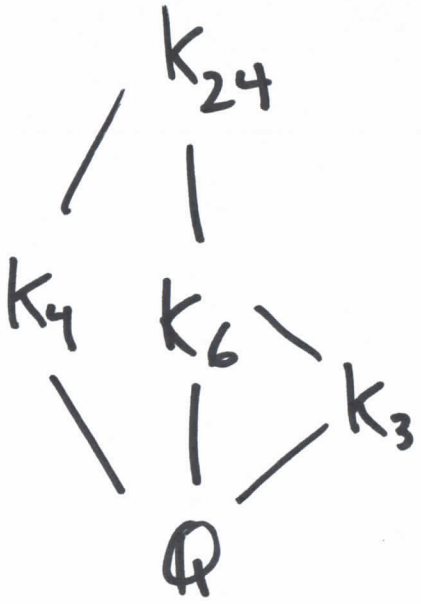
$\text{Gal}(K_6/K_3) \cong \mathbb{Z}/2\mathbb{Z}$

→ What do we need to know about K_4 in order to say that a prime ℓ is split completely in K_3?

→ How can we detect when K_6/K_3 is unramified in terms of K_4?

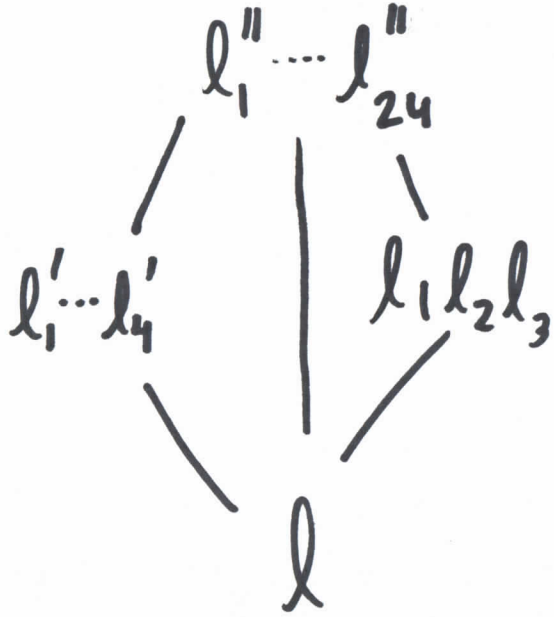
Decomposition Group	Inertia Group	Splitting Type in K_3	Splitting Type in K_4
(*) 1	1	(1, 1, 1)	(1, 1, 1, 1)
(12)	1	(1, 2)	(1, 1, 2)
(12)	(12)	$(1^2, 1)$	$(1, 1, 1^2)$
(*) (12)(34)	1	(1, 1, 1)	(2, 2)
(12)(34)	(12)(34)	(1, 1, 1)	$(1^2, 1^2)$
(123)	1	(3)	(1, 3)
(123)	(123)	(1^3)	$(1^3, 1)$
⋮	⋮	⋮	⋮

Now, we are ready to translate our global condition on K_3:



Case (i):

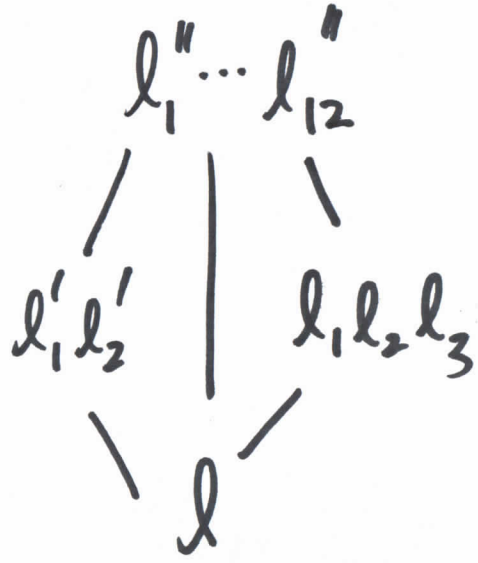
$\text{Frob}_\ell = 1$



$$\text{Frob}_{\ell_i} = \left(\frac{\ell_i}{K_6/K_3}\right) = 1, \forall i.$$

Case (ii):

$\text{Frob}_\ell = (12)(34)$



$$\text{Frob}_{\ell_1} = \left(\frac{\ell_1}{K_6/K_3}\right) = 1$$

$$\text{Frob}_{\ell_j} = \left(\frac{\ell_j}{K_6/K_3}\right) = -1, \; j = 2, 3.$$

By a theorem of Bhargava (2004) about counting quartic number fields, we obtain

THM: For a fixed rational prime ℓ, as we vary over S_3-cubic number fields in which ℓ splits completely into $\ell_1\ell_2\ell_3$, the $\mathbb{Z}/2\mathbb{Z}$-moment of case (i) is $\frac{1}{3}$ the $\mathbb{Z}/2\mathbb{Z}$-moment of case (ii).

Why might this happen?

Option 1:
(no ordering)

(0,0,0)
(1,1,0)

Option 2:
(ordering)

(0,0,0)
(0,1,1)
(1,0,1)
(1,1,0)

Our theorem supports the conjecture that if we restrict to S_3-cubic number fields K in which ℓ splits completely as $\ell_1\ell_2\ell_3$, then ℓ_1, ℓ_2, ℓ_3 are distributed as random ordered elements of $Cl(K)$.