Number fields $[K:\mathbb{Q}]<\infty$

How many number fields are there of deg d and $D_K := |\mathrm{Disc}\, K| \le X$?
(asymptotically)

$K/\mathbb{Q}$ $\tilde{K}$ Galois closure $\underbrace{\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \text{ acts on } \{K \to \tilde{K}\}}_{\text{permutation group}}$

Ques What are the asymptotics of

$$N_G(X) := \{ K/\mathbb{Q} \mid \mathrm{Gal}(\tilde{K}/\mathbb{Q}) = G, D_K \le X \} \ ?$$

First case: $G = C_2$, counting quadratic fields

How do we know quadratic fields?

Each generated by α w/ $\alpha^2 + a\alpha + b = 0$ $a,b \in \mathbb{Z}$

$\alpha^2 - d = 0$ $d \in \mathbb{Z}$ square-free

- These are all different.
- We can compute $D_K = d, 4d$

$\approx$ need to count square-free integers.

$N(X) = \{ D \ \square\text{-free} \in [1,X] \}$ $N_n(X) = \{ D = n^2 d \in [1,X] \}$

$$N(X) = N_1(X) - \sum_{\substack{p \\ \text{primes}}} N_p(X) + \sum_{p,q} N_{pq}(X) - \cdots$$

$$= \sum_n \mu(n) N_n(X)$$

$N_n(X) \neq 0 \Rightarrow n \le \sqrt{X}$

$$= \sum_{n \le \sqrt{X}} \mu(n) \left(\frac{X}{n^2} + O(1) \right)$$

$$= \sum_n \mu(n) \frac{X}{n^2} - \sum_{n > \sqrt{x}} \mu(n) \frac{X}{n^2} + O(\sqrt{x})$$

$$= X \prod_p (1 - p^{-2}) + O(\sqrt{x})$$

$$= \zeta(2)^{-1} X + o(X)$$

Also (see notes)

$$N_{C_2}(X) = \frac{X}{\zeta(2)} + o(X)$$

Next: higher degree?

$[K:\mathbb{Q}]=3$ generated by α: $f(\alpha)=\alpha^3+p\alpha+q=0$ $p,q\in\mathbb{Z}$

- When do 2 (p,q) give same field?
- What is discriminant of $\mathbb{Q}(\alpha)$?

$$D_K \mid \operatorname{disc}(f)$$

We can answer in individual cases, but not systematically enough to count. easily

Moral: isom. classes of fields $\not\leftrightarrow$ polynomials

Nonetheless:

- looking for algebraic numbers gives best general approach to tabulation of deg d fields

listing each field with $|D_K| \le X$ once

- w/ heuristics, can give conjecture for $N_{S_d}(X)$ [& unconditional $N_{S_3}(X)$]

Shankar–Tsimerman

- best upper & lower bounds $N_{S_d}(X)$
- much less access to $N_G(X)$ $G \subsetneq S_d$

Three Approaches to Count $N_G(X)$

① Class Field Theory

G abelian

(Cohn) $G = C_3$ $\qquad \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), C_3) \simeq \mathrm{Hom}(C_{\mathbb{Q}}, C_3)$

idele class group

$$\prod_p{}' \mathbb{Z}_p^* \times \mathbb{R}^*_{>0} \xrightarrow{\sim} C_{\mathbb{Q}}$$

$$\mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), C_3) \simeq \prod_p{}' \mathrm{Hom}(\mathbb{Z}_p^*, C_3)$$

kernel pro-p group

$p \neq 3 \quad \mathbb{Z}_p^* \to (\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z} \longrightarrow C_3$ $\qquad$ 2 non-trivial maps when $p \equiv 1 \pmod 3$

What is discriminant? (unramified @ 3)

$$D_K = \Big(\prod_{\substack{p \text{ s.t.} \\ \mathbb{Z}_p^* \to C_3 \text{ non-trivial}}} p\Big)^2$$

Analytic number theory: $D(s) = \sum_n a_n n^{-s}$

asymptotics of $\sum_{n \le X} a_n$ come from right-most poles of $D(s)$

$$D(s) = \sum_n n^{-s} \left\{ \begin{matrix} \# \text{ Homs} \\ D_K = n \end{matrix} \right\} = \prod_{p \equiv 1 \pmod 3} (1 + 2p^{-2s})$$

$$\zeta(2s) L(\chi, 2s) = \prod_{p \equiv 1 \pmod 3} (1 - p^{-2s})^{-2} \prod_{p \equiv 2 \pmod 3} (1 - p^{-4s})$$

* ignoring $p=3$ factors

χ: Dirichlet char mod 3

$$\frac{D(s)}{\zeta(2s) L(\chi, 2s)} = \prod_{p \equiv 1} (1 - 3p^{-4s} + 2p^{-5s}) \prod_{p \equiv 2} (1 - p^{-4s})$$

analytic for $\mathrm{Re}(s) > \frac{1}{4}$

So $D(s)$ rightmost pole @ $s = \frac{1}{2}$ like $\zeta(2s) L(\chi, 2s)$

$$\rightsquigarrow N_{C_3}(X) = c X^{1/2} + o(X^{1/2}).$$

Can count all abelian fields this way [Mäki, ...]

Also reasonable for tabulation

② Parametrizations & geometry of numbers

(Davenport-Heilbronn) $[K:\mathbb{Q}]=3$ $\quad \mathcal{O}_K \cong \mathbb{Z}^3$ $\quad \mathbb{Z}$-module basis $1, \omega, \theta$

$\omega \mapsto \omega + k \quad \theta \mapsto \theta + \ell$

$k, \ell \in \mathbb{Z}$

To determine $\mathcal{O}_K$:

$$\omega\theta = \underline{-ad} + \underline{0}\,\omega + \underline{0}\,\theta$$
$$\omega^2 = \underline{-ac} + \underline{-b}\,\omega + \underline{a}\,\theta$$
$$\theta^2 = \underline{-bd} + \underline{-d}\,\omega + \underline{c}\,\theta$$

$a, b \ldots \in \mathbb{Z}$

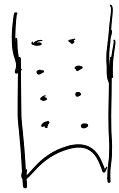
eqns of assoc $\Leftarrow$

So $\left\{ \begin{array}{l} \mathcal{O}_K \text{ w/ } \mathbb{Z}\text{-basis} \\ \text{of } \mathcal{O}_K/\mathbb{Z} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{some} \\ (a,b,c,d) \\ \in \mathbb{Z}^4 \end{array} \right\}$

A different basis of $\mathcal{O}_K/\mathbb{Z}$ $\rightsquigarrow$ a $GL_2(\mathbb{Z})$ action

Can work out explicitly
- $GL_2(\mathbb{Z}) \curvearrowright \mathbb{Z}^4$
- which $(a,b,c,d) \in \mathbb{Z}^4$ correspond to $\mathcal{O}_K$

Key: "generic" (a,b,c,d) correspond to $\mathcal{O}_K$

Count (a,b,c,d) in a fundamental domain 
to count one per orbit

Use geometry of numbers

$$\rightsquigarrow N_{S_3}(X) = \frac{1}{3\zeta(3)} X + o(X)$$

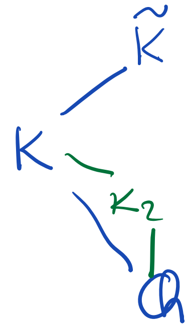
Gives very fast tabulation of cubic fields
(Belabas)

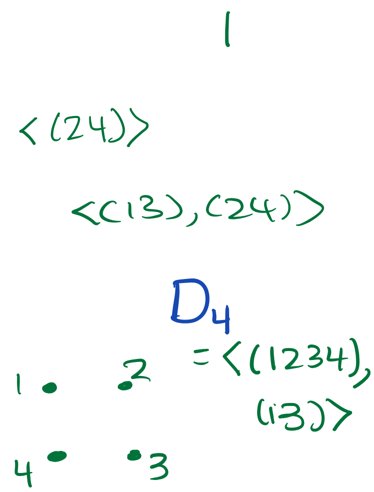
Potential for fast tabulation of quartic, quintic
using Bhargava's parametrizations

(3) Extensions of extensions

D_4-quartic extensions

(Cohen, Diaz y Diaz, Olivier)





$$N_{F,S_2}(X) = \{ [K:F]=2,\ Nm_{F/\mathbb{Q}}(\mathrm{Disc}\, K/F) \le X \}$$

K
/
F
\
$\mathbb{Q}$

K could be C_4, $C_2 \times C_2$, or D_4

these have already been counted

$$N(X) = \sum_{[F:\mathbb{Q}]=2} N_{F,S_2}\left(\frac{X}{D_F^2}\right)$$

$$D_K = Nm_{F/\mathbb{Q}}(\mathrm{Disc}\, K/F) \times D_F^2$$

$$= \sum_{[F:\mathbb{Q}]=2} \frac{C_F\, X}{D_F^2} + o(X)$$

use this to interchange w/ the sum.

Tail bound: $N_{F,S_2}(X) \le C\, D_F^{2/3} X$

$$N_Y(X) = \sum_{\substack{[F:\mathbb{Q}]=2 \\ D_F \le Y}} N_{F,S_2}\left(\frac{X}{D_F^2}\right) = \left(\sum_{\substack{F \\ D_F \le Y}} \frac{C_F}{D_F^2} \right) + o(X)$$

$$\liminf_{X\to\infty} \frac{N(X)}{X} \geq \sum_F \frac{C_F}{D_F^2}$$

$$N(X) \leq N_Y(X) + \sum_{\substack{F \\ D_F > Y}} N_{F,S_2}\left(\frac{X}{D_F^2}\right)$$

$$\leq N_Y(X) + \sum_{\substack{[F:\mathbb{Q}]=2 \\ D_F > Y}} C D_F^{-4/3} X$$

$\sum_{[F:\mathbb{Q}]=2} D_F^{-4/3}$ converges

$$\limsup_{X\to\infty} \frac{N(X)}{X} \leq \sum_F \frac{C_F}{D_F^2} + \lim_{Y\to\infty} \sum_{D_F > Y} C D_F^{-4/3}$$

$$N(X) = \left(\sum_{[F:\mathbb{Q}]=2} \frac{C_F}{D_F^2}\right) X + o(X) \rightsquigarrow N_{D_4}(X) = c_{D_4} X + o(X)$$

See notes for

- Conjectures
- More results
- Variations
- Suggested projects

Distribution of class groups of number fields

As K number field varies, what is distribution of Cl_K? $\underbrace{Cl_K[p^\infty]}_{\text{Sylow } p\text{-subgroup}}$?

$$\boxed{\lim_{X\to\infty} \frac{\#\{K/\mathbb{Q}\ G\text{-extn},\ D_K \le X,\ Cl_K[p^\infty] \cong A\}}{\#\{K/\mathbb{Q}\ G\text{-extn},\ D_K \le X\}}}$$

More generally,

$$\lim_{X\to\infty} \frac{\sum_{\substack{K\in\mathcal{F} \\ I_K \le X}} f(Cl_K)}{\sum_{\substack{K\in\mathcal{F} \\ I_K \le X}} 1}$$

"average" of f over Cl_K for $K\in\mathcal{F}$ by I_K ?

Start w/ quadratic fields

- Cl_K quite different for K imag vs. real

finitely many $Cl_K = 1$

infinitely many w/ $Cl_K = 1$???

What do we know? · Cl_K finite abelian group

- genus theory

Today: genus theory through class field theory

$$Cl_K = \mathrm{Gal}(K^{un,ab}/K)$$

maximal unramified, abelian extension

$$\begin{array}{ccc} & EK & \\ E & & K \\ & \mathbb{Q} & \end{array}$$

abelian (EK/K), abelian ($E/\mathbb{Q}$)

Genus field: maximal extn of K, unram, abelian, & EK for some $E/\mathbb{Q}$ $\underline{\text{abelian}}$

$EK \subset K^{un,ab}$

$$Cl_K \twoheadrightarrow \underbrace{Gal(EK/K)}_{\text{genus group}}$$

What can EK be?

$\underline{K \text{ quadratic field}}$

Class field theory $\Rightarrow Gal(EK/\mathbb{Q}) = Gal(EK/K) \rtimes \underset{\text{order } 2}{Gal(K/\mathbb{Q})}$

$\subset Gal(E/\mathbb{Q}) \times Gal(K/\mathbb{Q})$

So $Gal(EK/K)$ must be 2-torsion.

$$\begin{tikzcd}
 & L=FK \arrow[dl, dash] \arrow[dr, dash, "\text{unramified}"] & \\
F \arrow[dr, dash, "2"'] & & K \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
\langle(1,0)\rangle \arrow[d, dash] \\
\mathbb{Z}/2 \times \mathbb{Z}/2
\end{tikzcd}$$

Inertia $\cap \langle(1,0)\rangle = 1$

$$\begin{tikzcd}
Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[r, dashed] \arrow[dr] & Gal(L/\mathbb{Q}) \arrow[d, dashed] = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\
 & Gal(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}
\end{tikzcd}$$

Class field theory: $Hom(Gal(\overline{\mathbb{Q}}/\mathbb{Q}), A)$ $\quad$ A finite abelian

$\quad\quad = Hom(C_{\mathbb{Q}}, A)$ $\quad$ idele class group

$\quad\quad = Hom(\prod_p{}' \mathbb{Z}_p^*, A)$

$$\begin{tikzcd}
\prod_p \mathbb{Z}_p^* \arrow[r, dashed] \arrow[dr, "\text{corr to } K"'] & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \arrow[d] \\
 & \mathbb{Z}/2\mathbb{Z}
\end{tikzcd}$$

$\mathbb{Z}_p^*$ are inertia groups,

image can't intersect $(\langle 1,0\rangle)$ non-trivially

So p unram in $K \Rightarrow \mathbb{Z}_p^* \mapsto 1$

p ram in $K \Rightarrow$ 2 options of a lift

So $2^{\#\text{ram primes}}$ maps

- 2 not surjections
- Each field gives 2 maps
- Some may be ramified @ ∞

$$2^{\#\text{ram}} - 1 \geq |\underbrace{Gal(EK/K)}_{\text{genus group}}| \geq 2^{\#\text{ram primes of } K - 2}$$

genus group $\approx (\mathbb{Z}/2\mathbb{Z})^t$ some t

Moral: we know $Cl_K[2]$ for K quadratic

Cohen-Lenstra Heuristics

p odd prime

Conj For "reasonable" f

$$\lim_{X\to\infty} \frac{\sum_{\substack{K \text{ imag quad} \\ D_K \leq X}} f(Cl_K[p^\infty])}{\sum_{\substack{K \text{ imag quad} \\ D_K \leq X}} 1} = \frac{\sum_{\substack{A \text{ fin ab.} \\ p\text{-group}}} \frac{1}{|Aut(A)|} f(A)}{\sum_{\substack{A \text{ fin ab.} \\ p\text{-group}}} \frac{1}{|Aut A|}}$$

$$\lim_{X\to\infty} \frac{\sum_{\substack{K \text{ real quad} \\ D_K \leq X}} f(Cl_K[p^\infty])}{} = \frac{\sum_{\substack{A \text{ fin ab.} \\ p\text{-group}}} \frac{1}{|A|\,|Aut(A)|} f(A)}{}$$

$$\sum_{\substack{K \text{ real quad} \\ D_K \le X}} 1 \qquad\qquad \sum_{\substack{A \text{ fin ab.} \\ p\text{-group}}} \frac{1}{|A||\mathrm{Aut}\,A|}$$

Moral (Conj) A appears $\underbrace{\frac{c}{|\mathrm{Aut}\,A|}}_{\text{among imag quad}}$ or $\underbrace{\frac{c}{|A||\mathrm{Aut}\,A|}}_{\text{among real quad.}}$ of the time

Tables of class groups of quadratic fields both

- helped motivate these conjectures
- provided evidence for the conjectures

A Matrix Model

(Venkatesh–Ellenberg) $[K:\mathbb{Q}]=2$ $\quad S$ a finite set of primes of K sufficient to generate $\mathcal{C}\ell_K$

S-units $\quad \mathcal{O}_S^* = \{\alpha \in K \mid \mathrm{val}_{\mathfrak{p}}(\alpha)=0 \ \forall \mathfrak{p} \notin S\}$

S-ideals $\quad I_S$ fractional ideals generated by $\mathfrak{p} \in S$

μ_K roots of unity in K

$$M: \mathcal{O}_S^*/\mu_K \longrightarrow I_S$$

$$\alpha \longmapsto (\alpha)$$

$$\mathrm{cok}\, M = I_S / M(\mathcal{O}_S^*/\mu_K) = \mathcal{C}\ell_K$$

$$\mathcal{C}\ell_K[p^\infty] = \mathrm{cok}\, M_p : \mathcal{O}_S^*/\mu_K \otimes \mathbb{Z}_p \longrightarrow I_S \otimes \mathbb{Z}_p$$

Pick a $\mathbb{Z}$-module basis of

$$\mathcal{O}_S^*/\mu_k \simeq \begin{cases} \mathbb{Z}^{|S|} & \text{(imag)} \\ \mathbb{Z}^{|S|+1} & \text{(real)} \end{cases} \qquad I_S \simeq \mathbb{Z}^{|S|}$$

$M_p \in \mathrm{Mat}_{n \times n+u}(\mathbb{Z}_p)$ $\qquad u = 0, 1$

How might these be distributed?

Mod p?	uniform
Mod p^2?	uniform
⋮	⋮
Over $\mathbb{Z}_p$	Haar

A random matrix question

Take $N_p \in \mathrm{Mat}_{n \times n+u}(\mathbb{Z}_p)$ from Haar measure

What is distribution of cok N_p?

<u>Sketch</u>

$N_p : \mathbb{Z}_p^{n+u} \to \mathbb{Z}_p^n$

$$\mathbb{Z}_p^n / N_p \mathbb{Z}_p^{n+u} \simeq B$$

fixed abelian p-group

$|B|^n$ maps $\mathbb{Z}_p^n \xrightarrow{f} B$

Given one, what is prob f gives ?

- Prob $|B|^{-n-u}$ $\quad N_p \mathbb{Z}_p^{n+u} \subset \ker f$
- Compute prob $\quad$ generates ker (can be checked mod p by Nakyama's Lemma)

$$\lim_{n\to\infty} \mathrm{Prob}\left(\mathbb{Z}_p^n / N_p \mathbb{Z}_p^{n+u} \simeq B \right) = \frac{c_{p,u}}{|B|^u |\mathrm{Aut}\, B|}$$

$u=0$ Cohen-Lenstra dist. conj. for imag quad
$u=1$ " " real "

Maybe: (*) these $\mathcal{O}_S^*/\mu_K \otimes \mathbb{Z}_p \to I_S \otimes \mathbb{Z}_p$ are

$\approx$ distributed from Haar measure on $\mathrm{Mat}_{n \times n+u}(\mathbb{Z}_p)$?

Would $\Rightarrow$ Cohen-Lenstra distribution for quadratic fields.

Caveat: to even make sense of this, need basis for

$\mathcal{O}_S^*/\mu_K$.

Preliminary computations suggest (*) fails

Universality

Actually, many more distributions of random $M_p \in \mathrm{Mat}_{n\times n+u}(\mathbb{Z}_p)$ [not just from Haar measure!] have $\operatorname{cok} M_p \approx$ Cohen-Lenstra distribution

Take any distribution on $\mathbb{Z}_p$ not all same mod p.

(W.) $N_p \in \mathrm{Mat}_{n\times n+u}(\mathbb{Z}_p)$ entries i.i.d. from it

$$\lim_{n\to\infty} \mathrm{Prob}(\operatorname{cok}(N_p) \simeq B) = \frac{c}{|B|^u |\mathrm{Aut}\, B|}$$

Ques What is the distribution (empirically) of these M_p (defining class groups) and does this universality hold for that distribution?

Moments of Class Group Distributions

We are interested in averages

$$\lim_{X\to\infty} \frac{\displaystyle\sum_{\substack{K \text{ imag quad} \\ D_K \le X}} f(\mathrm{Cl}_K[p^\infty])}{\displaystyle\sum_{\substack{K \text{ imag quad} \\ D_K \le X}} 1} =: \mathcal{E}(f(\mathrm{Cl}_K[p^\infty]))$$

(p odd prime)

So far, mostly thought about $f = \mathbb{1}_B$ characteristic function of a finite abelian p-group.

Rmk Averages of $\mathbb{1}_B$'s don't determine other averages because of the limit.

Another important class of f: $f_B(X) = \#\mathrm{Sur}(X, B)$ (surj. homo.)

Average of $\#\mathrm{Sur}(-, B)$ is the B-moment of a distribution of groups

[Analogy: Average of x^k is kth-moment of a distribution of real numbers]

[Wang-W.) **Thm** Let X, Y be random finite abelian groups.

If for every finite abelian group B, we have

$$\int_X \#\mathrm{Sur}(X,B)\,d\mu = \mathbb{E}(\#\mathrm{Sur}(X, B)) = \mathbb{E}(\#\mathrm{Sur}(Y, B)) = O(|\wedge^2 B|)$$

then for every finite abelian group A,

$$\mathrm{Prob}(X \simeq A) = \mathrm{Prob}(Y \simeq A).$$

We are interested in limits of random variables/distributions.

Thm (W.) Let p be a prime. Let $Y, X_1, X_2, \ldots$ be random abelian p-groups. If for every abelian p-group B, we have

$$\lim_{n\to\infty} \mathbb{E}(\#\mathrm{Sur}(X_n, B)) = \mathbb{E}(\#\mathrm{Sur}(Y, B)) = O(|\wedge^2 B|)$$

then for every finite abelian group A,

$$\lim_{n\to\infty} \mathrm{Prob}(X_n \simeq A) = \mathrm{Prob}(Y \simeq A).$$

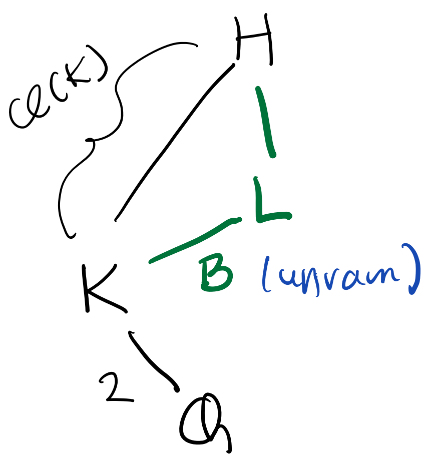
Moral Averages of $\#\mathrm{Sur}(-, B)$ over class groups for all B

$$\Downarrow$$

Averages of $\mathbb{1}_A$ over class groups for all A

Relationship of moments to field counting

$[K:\mathbb{Q}] = 2$ $\qquad$ H Hilbert class field of K $= K^{un,ab}$



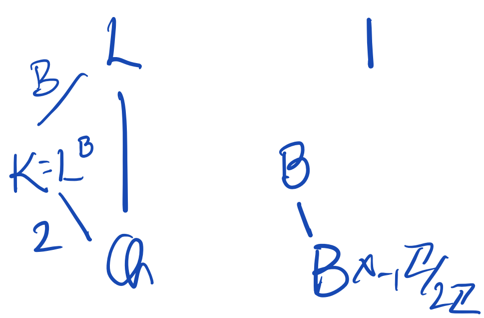
$\phi \in \mathrm{Sur}(\mathrm{Cl}(K), B)$

$\updownarrow$ (Galois theory)

L

Class field theory $\Rightarrow$

- $L/\mathbb{Q}$ Galois
- $\mathrm{Gal}(L/\mathbb{Q}) \simeq B \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$



Conversely, $L/\mathbb{Q}$ Galois, $\mathrm{Gal}(L/\mathbb{Q}) = B \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$

gives $K/\mathbb{Q}$ quadratic, L/K B-extension

L/K unram $\iff$ inertia in $\mathrm{Gal}(L/\mathbb{Q}) \cap B = 1$ ⊛

So Average of $\#\mathrm{Sur}(\mathrm{Cl}_K, B) = \dfrac{\#\{L/\mathbb{Q} \ B \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}\text{-extns (inertia conds, cond @ } \infty)\}}{\#\{K/\mathbb{Q} \text{ imag quad}\}}$

The only average $\mathcal{E}(f(\mathrm{Cl}_K[p^\infty]))$ we know uses this.

(Davenport-Heilbronn) **Thm** $\mathcal{E}(\#\mathrm{Sur}(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z})) = 1.$

K imag quad

$\mathbb{Z}/3\mathbb{Z} \rtimes_{-1} \mathbb{Z}/2\mathbb{Z} = S_3$ $\quad$ S_3 Galois extensions $\longleftrightarrow$ non-Galois cubics

+ imposing conditions on inertia

Thm as predicted by the (later) Cohen-Lenstra heuristics.

Indeed: $$\frac{\displaystyle\sum_{\substack{A \text{ abelian} \\ p\text{-group}}} \frac{\#\mathrm{Sur}(A,B)}{|\mathrm{Aut}(A)|}}{\displaystyle\sum_{\substack{A \text{ abelian} \\ p\text{-group}}} \frac{1}{|\mathrm{Aut}\,A|}} = 1$$ for all B abelian p-groups

Recall our matrix model $N \in \mathrm{Mat}_{n \times n}(\mathbb{Z}_p)$ from Haar measure?

$$\mathbb{E}(\#\mathrm{Sur}(\mathrm{cok}\, N, B))$$

$$= \mathbb{E}\left(\#\mathrm{Sur}\left(\mathbb{Z}_p^n / \underbrace{N\mathbb{Z}_p^n}_{\text{col space of } N}, B\right)\right)$$

$$= \sum_{\phi \in \mathrm{Sur}(\mathbb{Z}_p^n, B)} \mathrm{Prob}(N\mathbb{Z}_p^n \subset \ker \phi)$$

each column of N independent from Haar measure on $\mathbb{Z}_p^n$

$$= \sum_{\phi \in \mathrm{Sur}(\mathbb{Z}_p^n, B)} |B|^{-n}$$

$$= \frac{\#\mathrm{Sur}(\mathbb{Z}_p^n, B)}{|B|^n} \xrightarrow[n \to \infty]{} 1$$

This doesn't automatically give

$$\mathbb{E}\Big(\#\mathrm{Sur}\big(\underbrace{\lim_{n\to\infty} \mathrm{cok}\, N}_{\text{Cohen-Lenstra distribution}}, B\big)\Big) = 1$$

but w/ a converge theorem we can show $\Uparrow$.

Summary

$\forall\, B$,

$$\mathcal{E}(\#\mathrm{Sur}(\mathrm{Cl}_K[p^\infty], B)) = 1 \implies$$

$\forall\, A$ proportion of K with $\mathrm{Cl}_K[p^\infty] \simeq A$ is $\dfrac{c}{|\mathrm{Aut}\, A|}$

[But not vice versa!]

Next lecture • generalization to class groups of higher degree extns

class groups elements of quad fields $\longleftrightarrow$ (Dedekind) orbits of binary quad forms $\Rightarrow$ Very large tables of class groups of quadratic fields

$\Downarrow$

Cohen-Lenstra conjectures for quadratic fields look good

In higher degree, smaller tables + no conjectured speed of convergence

$\Longrightarrow$ challenges to using empirical evidence for conjectures.

Suggestion Would be good to have heuristics for

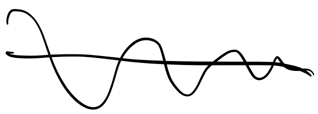
{ speed of convergence
error terms
secondary terms

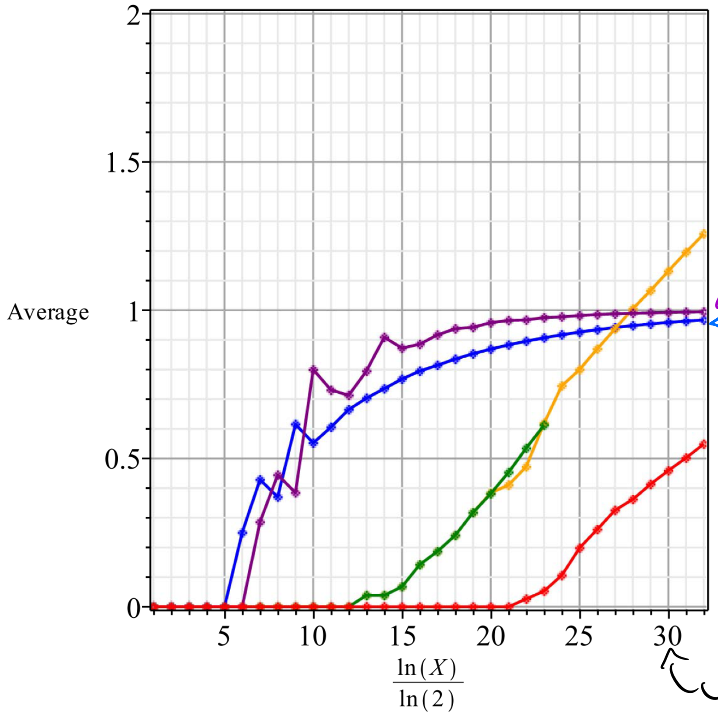
for quad fields

for Cohen-Lenstra conjectures. [where we are pretty confident in answer]

How does it depend on which moment/group?

in a way that could give insight for higher degree.





of imaginary quadratic fields

unramified A_4 extensions

$\mathbb{Z}/5\mathbb{Z}$-moment

$\mathbb{Z}/3\mathbb{Z}$-moment

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$-moment

up to $D_K \le 2^{30}$

Known secondary term

(Bhargava–Shankar–Tsimerman–Taniguchi–Thorne)

<u>Thm</u> $$\mathcal{E}(\#\mathrm{Sur}(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z})) = 1 - \underbrace{cX^{-1/6}}_{\text{secondary term}} + \overbrace{O(X^{-1/3+\varepsilon})}^{\text{error term}}$$

K imag quad

$c>0$ given explicitly

K real quad $$\frac{1}{3} - c' X^{-1/6} + O(X^{-1/3+\varepsilon})$$

Lewis-
Williams

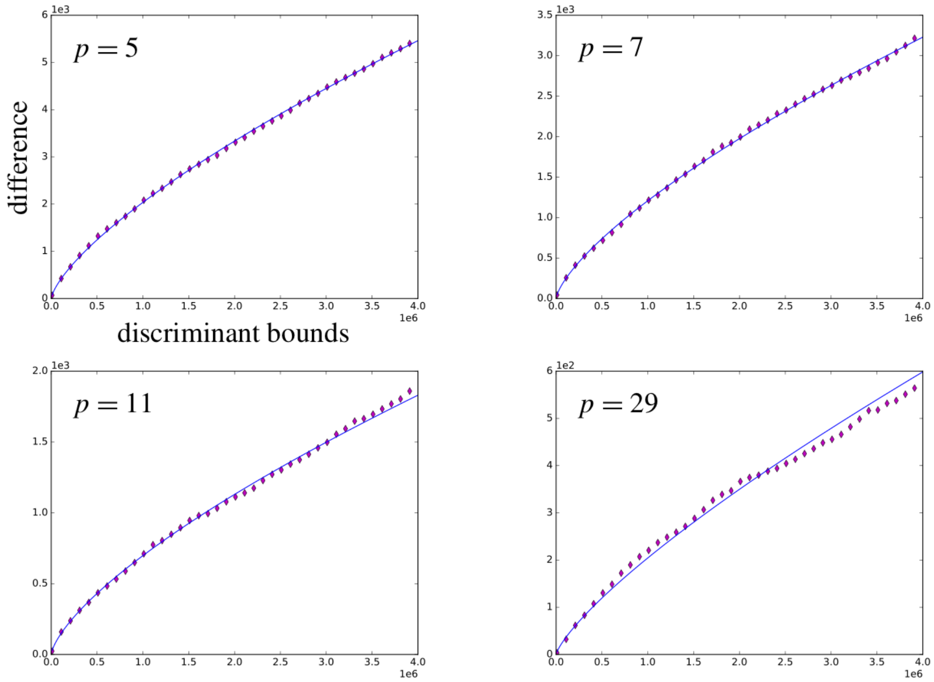


Figure 2. Plots of difference (3-1) with fitted curve from (3-2) for $p = 5, 7, 11$, and 29.

Follow-up from yesterday

Hough's paper "Equidistribution of Bounded Torsion CM pts"

gives theoretical heuristic suggesting

$$\mathcal{E}(\#\,\mathrm{Sur}(\mathcal{O}_K, \mathbb{Z}/k\mathbb{Z})) = 1 - cX^{-\frac{1}{2}+\frac{1}{k}} + o\left(X^{-\frac{1}{2}+\frac{1}{k}}\right)$$

K imag quad

k odd

$k=3$ $\quad -\frac{1}{2}+\frac{1}{3} = -\frac{1}{6}$

$k=5$ $\quad -\frac{1}{2}+\frac{1}{5} = \frac{-3}{10}$

Says for $k=5,7$ looks good w/ data

$k \geq 9$ looks not so good

Class Group Distributions for higher degree extensions

G finite group

$K/\mathbb{Q}$ Galois G-extn

$$Cl_K \text{ is a } \mathbb{Z}[G]\text{-module}$$

We should ask for its distribution as such.

[Thought experiment: What if the Cohen-Lenstra conjectures had been about only $|Cl_K|$?

Try to write $\displaystyle\sum_{|A|=n} \frac{1}{|A||\mathrm{Aut}\,A|}$ without mentioning groups.]

Cl_K as a $\mathbb{Z}[G]$-module

$N = \sum_{g \in G} g \in \mathbb{Z}[G]$ $\qquad N\, Cl_K[p^\infty] = 0$ $\qquad$ p prime, $p \nmid |G|$

Let p prime, $p \nmid |G|$

$R = \mathbb{Z}_p[G]/N$ $\qquad Cl_K[p^\infty]$ is an R-module.

$S_{G,G_\infty} = \{$ Galois G-extns $K/\mathbb{Q}$ w/ decomp group @ ∞ $G_\infty \}$

keeping track of conjugacy class in G of complex conjugation

Cohen and Martinet have conjectures which imply (see Wang - W.)

$p \nmid |G|$ and f a "reasonable" function of R-modules

$$\lim_{X \to \infty} \frac{\displaystyle\sum_{\substack{K \in S_{G,G_\infty} \\ D_K \le X}} f(Cl_K[p^\infty])}{\displaystyle\sum_{\substack{K \in S_{G,G_\infty} \\ D_K \le X}} 1} = \frac{\displaystyle\sum_{\substack{A \text{ p-group} \\ R\text{-module}}} \frac{f(A)}{|A^{G_\infty}||\mathrm{Aut}_R(A)|}}{\displaystyle\sum_{\substack{A \text{ p-group} \\ R\text{-module}}} \frac{1}{|A^{G_\infty}||\mathrm{Aut}_R(A)|}}$$

fixed elements

" $Cl_K[p^\infty]$ is distributed as a R-module with relative probabilities $\dfrac{1}{|A^{G_\infty}||\mathrm{Aut}_R(A)|}$ "

This distribution has moments

$$\mathbb{E}(\#\mathrm{Sur}_R(-,B)) = \frac{1}{|B^{G_\infty}|}$$

(Wang-W.) __Thm__ These moments determine a unique distribution. (of R-modules)

WARNING: These conjectures need some modifications.

① Malle: through empirical computations of class groups ...

- conjs wrong at $p=2$ (or replacing $\mathbb{Q}$ by K_0, when $p \mid |\mu_{K_0}|$ "roots of unity issues")

② Bartel-Lenstra: for some G, ordered by discriminant, a positive proportion of G-fields contain a fixed subfield.

- So replace D_K by an invariant that doesn't have this property (perhaps $\prod$ ram primes)

__Rmk__ For $p \nmid |\mu_{K_0}|$ + ordered by $\prod$ ram primes, Liu-W.-Zureick-Brown prove that conjectures hold over $K_0 = \mathbb{F}_q(t)$ with an (early) $q \to \infty$ limit.

Class group distributions of non-Galois extns

G finite group, H subgroup

$L/\mathbb{Q}$ Galois G-extension $\quad K = L^H$

For p prime $p \nmid |G|$

$$\mathrm{Cl}_K[p^\infty] \simeq \mathrm{Cl}_L[p^\infty]^H$$

So in principle, Cohen-Martinet conjectures for distribution of

$\mathrm{Cl}_L[p^\infty]$ as a G-module $\Longrightarrow$ $\mathrm{Cl}_K[p^\infty]$ as a p-group

$$\{G\text{-modules}\} \xrightarrow{A \mapsto A^H} \left\{\begin{matrix}\text{abelian}\\ \text{groups}\end{matrix}\right\}$$

In Wang-W. we work out what this pushforward is.

Easiest case

$G \curvearrowright G/H$ (cosets) $\rightsquigarrow G \curvearrowright \mathbb{C}^{G/H} = \mathrm{Ind}_H^G \mathbb{C}$

$V_{G,H} = \mathbb{C}^{G/H} / \mathbb{C}$

trivial G-repn

Case when $V_{G,H}$ is (absolutely) irreducible:

Cohen-Martinet conj $\Longrightarrow$ (p prime $p \nmid |G|$)

$$\lim_{X\to\infty} \frac{\sum_{\substack{L \in S_{G,G^\infty} \\ D_L \le X}} f(\mathrm{Cl}_{L^H}[p^\infty])}{\quad} = \frac{\sum_{\substack{A \text{ abelian} \\ p\text{-group}}} \frac{f(A)}{|A|^u |\mathrm{Aut} A|}}{\quad}$$

$L^H \nsim K$

$$\sum_{\substack{L \in S_{G,G_\infty} \\ D_L \le X}} 1 \qquad \sum_{\substack{A \text{ abelian} \\ p\text{-group}}} \frac{1}{|A|^u |\mathrm{Aut} A|}$$

where $u = \#$ cycles of G_∞ on G/H -1 = unit rank of L^H / K

$K = L^H$

$Cl_K[p^\infty]$ is distributed as an abelian group with relative probabilities
$$\frac{1}{|A|^u |\mathrm{Aut} A|}$$

This is distribution determined by
$$B\text{-moment} = |B|^{-u}$$

Same caveats (ROU, counting invt) apply

Takeaway When $V_{G,H} = \mathbb{C}^{G/H} / \mathbb{C}$ is irreducible, $Cl_{L^H}[p^\infty]$ has no additional structure.

Next when $V_{G,H}$ is reducible,

$Cl_{L^H}[p^\infty]$ has extra structure

Ex $G = D_4 = \langle (1234), (24) \rangle$ $H = \langle (24) \rangle$ ← index 4

1 • • 2

4 • • 3

$K = L^H$ is a quartic D_4-extn

$|\mathrm{Aut}(K)| = 2$

$\mathrm{Aut}(K) \curvearrowright Cl_K$

__Ex__ $G = A_5$ $H = \langle (123), (12)(45) \rangle$ (index 10)

L G-extn $K = L^H$ $|\mathrm{Aut}(K)| = 1$

but $V_{G,H}$ not irreducible

Let $e = \frac{1}{|H|} \sum_{h \in H} h \in R = \mathbb{Z}_p[G]/N$.

idempotent (not necessarily central)

$T = \underbrace{eRe}_{\text{ring}} \subset R$ (maximal order in Hecke algebra $\mathbb{Q}_p[H \backslash G / H]$)

$Cl_L[p^\infty]$ R-mod

If B is an R-module, $\leadsto Cl_L[p^\infty]^H = Cl_K[p^\infty]$

T naturally acts on B^H

B^H is a T-module

(using $p \nmid |G|$ makes this much simpler)

__Thm__ $T \simeq \mathbb{Z}_p$ iff $V_{G,H}$ is irreducible.

So we ask about dist of $Cl_{L^H}[p^\infty]$

as a T-module.

Cohen-Martinet $\Longrightarrow$ (p prime $p \nmid |G|$)

$$\lim_{X\to\infty} \frac{\displaystyle\sum_{\substack{L \in S_{G,G^\infty} \\ D_L \le X}} f(Cl_{L^H}[p^\infty])}{\displaystyle\sum_{\substack{L \in S_{G,G^\infty} \\ D_L \le X}} 1} = \frac{\displaystyle\sum_{\substack{B \text{ } p\text{-gp} \\ T\text{-module}}} \frac{f(B)}{|(Re \otimes_T B)^{G_\infty}| \, |Aut_T B|}}{\displaystyle\sum_{\substack{B \text{ } p\text{-gp} \\ T\text{-module}}} \frac{1}{|(Re \otimes_T B)^{G_\infty}| \, |Aut_T B|}}$$

$Cl_K[p^\infty]$ is distributed as a T-module with relative probabilities

$$\frac{1}{|(Re \otimes_T B)^{G_\infty}| \, |Aut_T B|}$$

It would be great to have computational evidence for (or against!) these predictions

Many specific suggestions in notes, especially

- around the "caveats" + corrections
- in cases where no prediction is made ($p \mid |G|$)

sometimes Cohen-Martinet makes a prediction & sometimes not

Further

when $p \mid |G|$ more to say

Alex Smith determined distribution of $Cl_K[\ell^\infty]$ for C_ℓ-extns

cyclic group of order ℓ

(see his webpage for seminar announcement)
asmith-math.org