Melanie Wood (Wisconsin): Averages of p-torsion in class groups over function fields - good and bad primes

$K/\mathbb{Q}$ imag. quad., $K = \mathbb{Q}(\sqrt{-D})$, $D > 0$ sq. free

Class group $Cl(K)$

For prime p, the p-torsion subgp. is

$$Cl_K[p] \simeq (\mathbb{Z}/p\mathbb{Z})^{d_p} \quad \text{for some } d_p \geq 0$$

$d_p = d_p(K)$, $|Cl_K[p]| = p^{d_p}$

Qn: How does d_p behave as K varies?

View as a random variable (depending on K)

$\mathbb{E}(\quad) = ?$ k-th moments

$(p^{d_p})^k$

Choose K uniformly from truncated listing:

$$\lim_{X\to\infty} \frac{\sum_{|\mathrm{disc}K|\leq X} (p^{d_p})^k}{\#\{K \mid |\mathrm{disc}\, K| \leq X\}}$$

Genus theory applies to 2-torsion

$$Cl[2] \simeq (\mathbb{Z}/2\mathbb{Z})^{\#\text{ ramified } p - 1}$$

$$\Rightarrow \mathbb{E}(2^{d_2}) = \infty$$

Conj: (Cohen-Lenstra 1984) p odd $\Rightarrow \mathbb{E}(|Cl_K[p]|) = 2$

Thm: (Davenport-Heilbronn 1971) True for $p = 3$

- 2 is "bad", 3, 5, 7 are "good"

- Slightly different for real quad. $K/\mathbb{Q}$:

$$\mathbb{E}(|Cl_K[2]|^k) = \infty \quad \text{(Now w/ narrow class gp. as well)}$$

Conj: (Cohen-Lenstra)

$$\mathbb{E}(|Cl_K[p]|) = 1 + 1/p$$

- Davenport-Heilbronn: $p = 3$ case

Qn: For higher deg. $K/\mathbb{Q}$, which p are "bad" or "good"?

Cohen-Martinet 1990: Predicted bad, & good p in general

↑ All other p, where machinery breaks down

↑ Those p which were described by the heuristic machinery

Ex: If $K/\mathbb{Q}$ deg. 3, initially predicted $p=3$ bad, $p \neq 3$ good.

- Revisited in 1994: Data suggested some "good primes are not so good".

Conj (Cohen-Martinet) $K/\mathbb{Q}$ totally real, cubic,

$$p \neq 3 \quad \mathbb{E}(|Cl_K[p]|) = 1 + 1/p^2$$

Thm (Bhargava 2005) $p=2$ case is true

(So 2 is good?)

Some arguments suggest conj. true for $p=3$ too!

Malle 2010: Conjectures are numerically off when $\mathbb{Q}$ is replaced by a base field w/ p^{th} roots of 1.

Goal: Prove theorems when $\mathbb{Q}$ is replaced by fn. field $\mathbb{F}_q(t)$.

Strong analogy:

$$\mathbb{Z} \subseteq \mathbb{Q}$$

$$\mathbb{F}_q[t] \subseteq \mathbb{F}_q(t)$$

↑ Advantage: Many choices for q, all analogous to $\mathbb{Q}$, can even let $q \to \infty$.

Consider cubic extension

$$\begin{array}{ccc} K & \supseteq & C_{\mathbb{F}_q} \\ \deg. 3 \,\big| & & \downarrow 3\text{-}1 \text{ map} \\ \mathbb{F}_q(t) & & \mathbb{P}^1(\mathbb{F}_q) \end{array}$$

e.g. $\mathbb{F}_q(t)\left(\sqrt[3]{t^7+t+1}\right) = \mathbb{F}_q(t)[u]/(u^3 = t^7+t+1)$

$$\Big|$$

$$\mathbb{F}_q(t)$$

Measure extensions by discriminant norms

$$N_m\left(\text{Disc } K/\mathbb{F}_q(t)\right) = q^n$$

Given such an n, the possible K are the $\mathbb{F}_q$ points of a moduli space of curves. (and so have the availability of geometric structure)

Similarly for class gps.

Achter (2006) $q \to \infty$ result for class gps. of quadratic K.

Remark: Subtlety in limits, since $n \to \infty$ as well when counting class gps. Easier to let $q \to \infty$ first.

Ellenberg-Venkatesh-Westerland (2016): $n \to \infty$, then $q \to \infty$

Indeed, if $q \to \infty$ before $n \to \infty$, reduces to a question about components of moduli space.

i.e. H_0 only

For $n \to \infty$ first (EVW 16), need "stable homology" results.

Work in progress: "unstable" components

Thm: (W.) Given n, let $C_{n,q}$ be the set of "totally real" (split completely at ∞) cubic extns. $K/\mathbb{F}_q(t)$, with $\mathrm{Nm}(\mathrm{Disc}\, K/\mathbb{F}_q(t)) = q^n$

Then $$\lim_{n\to\infty} \lim_{\substack{q\to\infty \\ (q,p)=1 \\ \text{and } (q-1,p)=1 \text{ for } p \text{ odd}}} \mathbb{E}\left(|\mathcal{Cl}_K[p]| : K \in C_{n,q}\right) = 1 + 1/p^2$$

- Verifying Cohen-Martinet!

$$\lim_{n\to\infty} \lim_{q\to\infty} \mathbb{E}\left(|\mathcal{Cl}_K[p]|^2 : K \in C_{n,q}\right) = \begin{cases} 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^4} & p \geq 3 \\ 1 + \frac{1}{2} + \frac{1}{2^2} + \boxed{\frac{2}{2^4}} & p = 2 \end{cases}$$

This is expected due to 2nd roots of 1

$$\mathrm{Disc}\, K/\mathbb{F}_q(t) = \underbrace{\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_k}_{\text{Partially ramified}} \underbrace{\mathfrak{p}_{k+1}^2 \cdots \mathfrak{p}_m^2}_{\text{Totally ramified}}$$

Let $C'_{n,q} \subseteq C_{n,q}$ with $\mathrm{Disc}\, K/\mathbb{F}_q(t)$ not squarefree

Note: Proportion of sq. free elements in $\mathbb{F}_q[t] = 1$, so we are ignoring those K w/ non sq. free Disc.

Thm $\lim_{n\to\infty} \lim_{q\to\infty} \mathbb{E}\left(|Cl_K[3]| : K \in C_{n,q}^-\right) = 1 + 1/3$

The ramified primes are "pushed out" too far to be counted.
In fact, if K are ordered by product of ramified primes,
limit is ∞!

Takeaway: More 3-torsion in cubic extensions when more totally ramd. primes.

- For degree n, S_n extns., $p=2$ always needs ± 1 correction
  $p \mid n$ bad,
  $p \nmid n$ good.
- For $n\to\infty$, $q\to\infty$, EVW have baseline conjectures