Average of 3-torsion in class groups of 2-extensions

Jiuya Wang
Duke University
joint with Robert J. Lemke Oliver and Melanie M. Wood

MIT, Nov 17, 2020

Cohen-Lenstra Heuristic

Conjecture (Cohen-Lenstra Heuristics)

Given an odd prime ℓ and $k > 0$. Denote $\mathcal{F}_2$ to be the set of quadratic extensions. Then

$$\lim_{X\to\infty} \frac{\sum_{F\in\mathcal{F}_2(X)} |\mathrm{Cl}_F[\ell]|^k}{\sum_{F\in\mathcal{F}_2(X)} 1} = C_{k,\ell}.$$

Cohen-Lenstra Heuristic

Conjecture (Cohen-Lenstra Heuristics)

Given an odd prime ℓ and $k > 0$. Denote $\mathcal{F}_2$ to be the set of quadratic extensions. Then

$$\lim_{X\to\infty} \frac{\sum_{F\in\mathcal{F}_2(X)} |\mathrm{Cl}_F[\ell]|^k}{\sum_{F\in\mathcal{F}_2(X)} 1} = C_{k,\ell}.$$

Theorem (Davenport-Heilbroon)

Let $\ell = 3$ and $k = 1$. Then

$$\lim_{X\to\infty} \frac{\sum_{F\in\mathcal{F}_2(X)} |\mathrm{Cl}_F[\ell]|^k}{\sum_{F\in\mathcal{F}_2(X)} 1} = C_{k,\ell}.$$

Generalizations

Conjecture (Cohen-Martinet Heuristics)

Given a transitive permutation group $G \subset S_n$ and a good prime ℓ and $k > 0$. Denote $\mathcal{F}_G$ to be the set of G-extensions. Then

$$\lim_{X \to \infty} \frac{\sum_{F \in \mathcal{F}_G(X)} |\mathrm{Cl}_F[\ell]|^k}{\sum_{F \in \mathcal{F}_G(X)} 1} = C_{G,k,\ell}.$$

Generalizations

Conjecture (Cohen-Martinet Heuristics)

Given a transitive permutation group $G \subset S_n$ and a good prime ℓ and $k > 0$. Denote $\mathcal{F}_G$ to be the set of G-extensions. Then

$$\lim_{X\to\infty} \frac{\sum_{F\in\mathcal{F}_G(X)} |\mathrm{Cl}_F[\ell]|^k}{\sum_{F\in\mathcal{F}_G(X)} 1} = C_{G,k,\ell}.$$

Theorem (Bhargava)

Let $G = S_3 \subset S_3$, $\ell = 2$ and $k = 1$. Then

$$\lim_{X\to\infty} \frac{\sum_{F\in\mathcal{F}_G(X)} |\mathrm{Cl}_F[\ell]|^k}{\sum_{F\in\mathcal{F}_G(X)} 1} = C_{G,k,\ell}.$$

Generalizations

Conjecture (Gerth's Modification)

Given $G = C_p$, $\ell > 0$ and $k > 0$. Denote $\mathcal{F}_G$ to be the set of G-extensions. Then

$$\lim_{X\to\infty} \frac{\sum_{F\in\mathcal{F}_G(X)} |(p\,\mathrm{Cl}_F)[\ell]|^k}{\sum_{F\in\mathcal{F}_G(X)} 1} = C_{k,\ell}.$$

Generalizations

Conjecture (Gerth's Modification)

Given $G = C_p$, $\ell > 0$ and $k > 0$. Denote $\mathcal{F}_G$ to be the set of G-extensions. Then

$$\lim_{X\to\infty} \frac{\sum_{F\in\mathcal{F}_G(X)} |(p\,\mathrm{Cl}_F)[\ell]|^k}{\sum_{F\in\mathcal{F}_G(X)} 1} = C_{k,\ell}.$$

Theorem (Smith)

Let $G = C_2$, $\ell = 2^r$ and $k = 1$. Then

$$\lim_{X\to\infty} \frac{\sum_{F\in\mathcal{F}_G(X)} |(2\,\mathrm{Cl}_F)[\ell]|}{\sum_{F\in\mathcal{F}_G(X)} 1} = C_{k,\ell}.$$

Fouvry-Klüners, Klys, Koyman-Pagano...

Main Theorem

Theorem (Lemke-Oliver, W. , Wood)

Let $\mathcal{F}_n$ be the set of 2-extensions with degree n. Then there exists $C_n > 0$ such that

$$\lim_{X\to\infty} \frac{\sum_{K\in\mathcal{F}_n(X)} h_3(K)}{\sum_{K\in\mathcal{F}_n(X)} 1} = C_n.$$

Theorem (Lemke-Oliver, W. , Wood)

Let $\mathcal{F}_G$ be the set of G-extensions where G is a transitive permutation 2-group with a transposition. Then there exists $C_G > 0$ such that

$$\lim_{X\to\infty} \frac{\sum_{K\in\mathcal{F}_G(X)} h_3(K)}{\sum_{K\in\mathcal{F}_G(X)} 1} = C_G.$$

2-extensions

Lemma

Given a field extension L/k. The Galois group $\mathrm{Gal}(\tilde{L}/k)$ is a p-group if and only if L/k can re realized as a successive tower of relative C_p extensions

$$L = L_0 \supset L_1 \supset \cdots \supset L_n = k.$$

Therefore quartic 2-extensions :

Denominator

Theorem (Malle's Conjecture for 2-groups)

Let $G \subset S_n$ be a transitive permutation 2-group. If G contains a transposition, there exists $D_G > 0$ such that

$$N_k(G, X) \sim D_G X,$$

otherwise,

$$N_k(G, X) = O(X^{1/2+\epsilon}).$$

This follows from the work of Cohen-Diaz y diaz-Olivier, Klüners-Malle, Klüners, Albert.

Numerator

The summation that we would like to determine is :

$$N(X) = \sum_{F/\mathbb{Q}} h_3(F) \sum_{L/F, \mathrm{Disc}(L) \leq X} h_3(L/F)$$

$$= \sum_{F/\mathbb{Q}} h_3(F) \cdot \left(2N_F^{\mathrm{sf}}(S_3, \frac{X}{\mathrm{Disc}^2(F)}) + N_F(S_2, \frac{X}{\mathrm{Disc}^2(F)})\right)$$

So it naturally lead to understanding enumerating S_3 cubic extensions over a general number field.

Datskovsky-Wright

Theorem (Datskovsky-Wright, Bhargava-Shankar-Wang)

Let k be a number field. Then

$$\sum_{\substack{[F:k]=2 \\ |\mathrm{Disc}(F/k)|\leq X}} h_3(F/k) \sim X \cdot \frac{\mathrm{Res}_{s=1}\zeta_k(s)}{2^{r_2(k)}\zeta_k(2)} \cdot \left(1 + \frac{2^{r_1(k)}}{3^{r_1(k)+r_2(k)}}\right),$$

where $r_1(k)$ denotes the number of real places of k, $r_2(k)$ the number of pairs of complex places.

Two Limit Process

The natural idea is to use finite summation over F to approximate

$$N_Y(X) := \sum_{F/\mathbb{Q}, \mathrm{Disc}(F) \leq Y} h_3(F) \sum_{L/F, \mathrm{Disc}(L) \leq X} h_3(L/F).$$

Our goal is

$$\lim_{Y \to \infty} \lim_{X \to \infty} \frac{N_Y(X)}{X} = \lim_{X \to \infty} \lim_{Y \to \infty} \frac{N_Y(X)}{X}$$

Tail Estimate

Now we write

$$\frac{N(X)}{X} = \frac{N_Y(X)}{X} + \frac{N(X) - N_Y(X)}{X},$$

in order to commute the two limit processes, it suffices to show that the tail

$$\lim_{Y \to \infty} \lim_{X \to \infty} \frac{N(X) - N_Y(X)}{X} = 0$$

Q : What is the dependence on $\mathrm{Disc}(k)$ for $N_k(S_3, X)$?

Hypothetical Computation

Suppose $N_k(S_3, X) \ll_{[k:\mathbb{Q}],\epsilon} \mathrm{Disc}(k)^{\alpha} X$, then

$$N(X) - N_Y(X) \ll \sum_{\substack{[F:\mathbb{Q}]=2 \\ \mathrm{Disc}(F)\geq Y}} h_3(F) \cdot \mathrm{Disc}^{\alpha}(F) \cdot \frac{X}{\mathrm{Disc}(F)^2}$$

$$= X \sum_{\substack{[F:\mathbb{Q}]=2 \\ \mathrm{Disc}(F)\geq Y}} h_3(F) \cdot \mathrm{Disc}^{\alpha-2}(F)$$

Our goal : $\alpha < 1$!

Class Field Theory

For any number field k, by class field theory denote $C_k = \mathbb{A}_k^\times / k^\times$ to be the idèle class group

$$1 \to O_k^\times \to \prod O_{\mathfrak{p}}^\times \to C_k \to \mathrm{Cl}(k) \to 1.$$

Therefore

$$0 \to \mathrm{Hom}(\mathrm{Cl}_k, C_2) \to \mathrm{Hom}(C_k, C_2) \to \mathrm{Hom}(\prod O_{\mathfrak{p}}^\times, C_2),$$

So altogether we get

$$N_k(C_2, X) = O(h_2(k)\,\mathrm{Disc}(k)^\epsilon X).$$

Class Field Theory

Lemma

Given a relative extension F/k of number fields. The relative class group is trivially bounded by $|\mathrm{Cl}_{F/k}| \ll_{[F:\mathbb{Q}],\epsilon} \frac{\mathrm{Disc}(F)^{1/2+\epsilon}}{\mathrm{Disc}(k)^{1/2+\epsilon}}$.

The number of S_3 cubic field with $\mathrm{disc}(K/k) = n$ is bounded by

$$h_2(k) \cdot h_3(F/k) \ll h_2(k) \cdot \mathrm{Disc}(k)^{1/2+\epsilon} \cdot |n|^{1/2+\epsilon},$$

therefore we get the following trivial bound

Theorem (S)

For any number field k, we have

$$N_k(S_3, X) = O_{[k:\mathbb{Q}],\epsilon}(h_2(k)\,\mathrm{Disc}(k)^{1/2+\epsilon} X^{3/2+\epsilon}).$$

Shintani zeta Function

Shintani zeta function $\xi_k(s)$ is the generating series of cubic rings with non-zero discriminant. Given a signature α,

$$\xi_{k,\alpha}(s) := \sum_{\substack{R/\mathcal{O}_k: \\ \mathrm{Disc}(R/\mathcal{O}_k)\neq 0, \\ \mathrm{sgn}(R)=\alpha}} \frac{|\mathrm{Aut}(R)|^{-1}}{\mathrm{Disc}(R/\mathcal{O}_k)^s}.$$

We know quite a lot about them from Datskovsky-Wright :

- Poles ($s = 1$ and $s = 5/6$) and Residues
- Meromorphic Continuation
- Functional Equation involving $\hat{\xi}_{k,\beta}(s)$ for all signature β.

Cubic Rings vs Cubic Fields

- Cubic fields give a subset of cubic rings
- Cubic fields (cubic ètale algebras) generate cubic rings
  The generating series of cubic rings associated to A is

$$\zeta_k(4s)\zeta_k(6s-1)\frac{\zeta_A(2s)}{\zeta_A(4s)}$$

where

$$\zeta_A(s) = \begin{cases} \zeta_k(s)^3, & \text{if } A \simeq k^3, \\ \zeta_k(s)\zeta_F(s), & \text{if } A \simeq F \times k, \\ \zeta_K(s), & \text{if } A \simeq K, \end{cases}$$

for any cubic ètale algebra A.

Contour Integration

Using Perron's formula, we take a smoothing function $\phi(x) = e^{1-x}$ and shift the integral to $Re(s) = -1/2 + \epsilon$,

$$N_{k,\alpha}^3(X) \ll_\phi \sum_{\substack{0<\mathrm{Disc}(R/\mathcal{O}_k) \\ \mathrm{sgn}(R)=\alpha}} \frac{\phi(\mathrm{Disc}(R/\mathcal{O}_k)/X)}{|\mathrm{Aut}(R)|}$$

$$= \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \xi_{k,\alpha}(s)\Phi(s)X^s\,ds$$

$$= Res(\xi_{k,\alpha}(s)\phi(s)X^s)_{s=1} + Res(\xi_{k,\alpha}(s)\phi(s)X^s)_{s=5/6}$$

$$+ \frac{1}{2\pi i}\int_{-1/2-\epsilon-i\infty}^{-1/2-\epsilon+i\infty} \xi_{k,\alpha}(s)\Phi(s)X^s\,ds$$

Contour Integration

Applying the functional equation

$$\frac{1}{2\pi i}\int_{3/2+\epsilon-i\infty}^{3/2+\epsilon+i\infty} g(s)^{[k:\mathbb{Q}]}\cdot \mathrm{Disc}(k)^{4s-2}\hat{\xi}(s)\Phi(1-s)X^{1-s}\,ds$$

where $g(s)$ is uniformly bounded by a constant on $Re(s) = 3/2 + \epsilon$ and $\hat{\xi}(s) \ll \xi(s)$.

Lemma

For any s with $Re(s) > 3/2$, we have

$$\xi_{k,\alpha}(s) \ll_{[k:\mathbb{Q}],\epsilon} h_2(k)\,\mathrm{Disc}(k)^{1/2+\epsilon}.$$

Contour Integration

Theorem (L)

For any number field k and $X \geq 1$, we get the number of cubic rings with discriminant bounded by X is

$$N_k^3(X) \ll_{[k:\mathbb{Q}],\epsilon} X \cdot \mathrm{Res}_{s=1}\zeta_k(s) + X^{-1/2-\epsilon} h_2(k)\mathrm{Disc}(k)^{9/2+\epsilon},$$

in particular when $X \geq \mathrm{Disc}(k)^3 h_2(2/3)$ we have

$$N_k^3(X) = O_{[k:\mathbb{Q}],\epsilon}(\mathrm{Disc}(k)^{\epsilon} X).$$

Now comparing with the T-bound, we get for all $X \geq 1$.

$$N_k(S_3, X) \ll_{[k:\mathbb{Q}],\epsilon} h_2(k)\,\mathrm{Disc}(k)^{3/2+\epsilon} X.$$

Propogation of Orders

Lemma

The cubic rings associated to a single quadratic fields F/k has generating series

$$\sum_{R\in\mathcal{R}(F)} \frac{|\mathrm{Aut}(R)|^{-1}}{\mathrm{Disc}(R/\mathcal{O}_k)^s} = \frac{h_3(F/k)}{2\mathrm{Disc}(F/k)^s}\zeta_k(2s)\zeta_k(6s-1)\sum \frac{1}{|\mathfrak{a}|^{2s}},$$

where the summation is over all ideals in O_F that is trivial in $\mathrm{Cl}_F \,/\, \mathrm{Cl}_F^3 \cdot \mathrm{Cl}_k$.

Therefore for each quadratic field F, the contribution in $N_k^3(X)$ is at least $h_3(F/k)Z((\frac{X}{\mathrm{Disc}(F)})^{1/2})$.

Theorem (M)

Let k a number field and let $X \geq 1$. We have

$$N_k(S_3, X) \ll_{[k:\mathbb{Q}],\epsilon} D_k^{\epsilon} X^{1/2} \max\left\{ \frac{D_k^{3/2} h_2(k)^{1/3}}{(\mathrm{Res}_{s=1}\zeta_k(s))^{1/3}}, \frac{X^{1/2} D_k^{1/2}}{\mathrm{Res}_{s=1}\zeta_k(s)} \right\}.$$

We now compare with T-bound and S-bound and get the following bound

$$N_k(S_3, X) = O_{[k:\mathbb{Q}],\epsilon}(\mathrm{Disc}(k)^{1+\epsilon} h_2(k)^{2/3} X).$$

Now notice that for 2-extensions, we apply genus theory to get $h_2(k) \ll_{[k:\mathbb{Q}],\epsilon} \mathrm{Disc}(k)^{\epsilon}$. Now we are only ϵ away from what we need !

Non-trivial Bound for Class Numbers

Q : How do we bound **relative class numbers** non-trivially ?

Lemma (Ellenberg-Venkatesh)

Given a relative extension L/K with $[L:K] = d$, an integer $\ell \geq 1$ and $0 < \theta < \frac{1}{2\ell(d-1)}$. Denote M to be the number of prime ideals $p \subset O_K$ with $\mathrm{Nm}_{K/\mathbb{Q}}(p) < \mathrm{Disc}(L/K)^{\theta}$ that are split in L/K, then

$$|\mathrm{Cl}_L[\ell]| = O_{[L:\mathbb{Q}],\epsilon}\left(\frac{\mathrm{Disc}(L)^{1/2+\epsilon}}{M}\right).$$

Arakelov Class Group

Relative Arakelov Class Group

Lemma

Given a relative extension L/K with $[L:K] = d$,we have

$$\mathrm{Vol}(\widetilde{\mathrm{Cl}}_{L/K}) \ll_{[L:\mathbb{Q}],\epsilon} \mathrm{Disc}(L/K)^{1/2+\epsilon}\,\mathrm{Disc}(K)^{(d-1)/2+\epsilon}.$$

Relative Ellenberg Venkatesh

Lemma (Relative Ellenberg-Venkatesh)

Given a relative extension L/K with $[L:K] = d$, an integer $\ell \geq 1$ and $0 < \theta < \frac{1}{4\ell(d-1)}$. Denote M to be the number of prime ideals $p \subset O_K$ with $\mathrm{Nm}_{K/\mathbb{Q}}(p) < \mathrm{Disc}(L/K)^{\theta}$ that are split in L/K, then

$$|\mathrm{Cl}_{L/K}[\ell]| = O_{\epsilon,[K:\mathbb{Q}]}\left(\frac{\mathrm{Disc}(L/K)^{1/2+\epsilon}\,\mathrm{Disc}(K)^{(d-1)/2+\epsilon}}{M}\right).$$

Zero Density Estimate

On average, we do get a lot of small split primes for most quadratic extensions.

Theorem (Lemke Oliver–Thorner)

Let k be a number field, and for any ray class character χ of k, let $N_\chi(\sigma, T) := \#\{\rho : L(\rho, \chi) = 0, \Re(\rho) \in (\sigma, 1), |\Im(\rho)| \leq T\}$. Then there is a constant $c = c([k : \mathbb{Q}]) > 0$, such that for any $Q, T > 1$, any $1/2 \leq \sigma < 1$, and any $\epsilon > 0$

$$\sum_{|\mathfrak{q}| \leq Q} \sum_{\chi} N_\chi(\sigma, T) \ll_{[k:\mathbb{Q}],\epsilon} (\mathrm{Disc}(k) QT)^{c(1-\sigma)+\epsilon}.$$

Theorem I

Finally using this non-trivial bound on the critical range i.e. $X \sim \mathrm{Disc}(F)$, and a careful induction argument to all 2-extensions, we are ready to state the following theorem.

Theorem (Lemke-Oliver, W. , Wood)

Let $\mathcal{F}_n$ be the set of 2-extensions with degree n. Then there exists $C_n > 0$ such that

$$\lim_{X\to\infty} \frac{\sum_{K\in\mathcal{F}_n(X)} h_3(K)}{\sum_{K\in\mathcal{F}_n(X)} 1} = C_n.$$

Thin Family

Recall that for a transitive permutation 2-group G :

- G contains a transposition $\iff$ $N(G, X) \sim CX$ $\iff$ $G \simeq C_2 \wr H$ for some 2-group H
- G does not contain a transposition $\iff$ $N(G, X) = O(X^{1/2+\epsilon})$

Thin Family

Theorem

Given a transitive permutation 2-group $G \subset S_n$ without a transposition. Denote $\mathcal{F}_G$ to be the set of isomorphism classes of G-extensions over k. Then there exists $\delta > 0$ such that

$$\sum_{K \in \mathcal{F}_G(X)} |\mathrm{Cl}_K[3]| = O(X^{1-\delta}).$$

Theorem II

Theorem (Lemke-Oliver, W. , Wood)

Let $\mathcal{F}_G$ be the set of G-extensions where G is a transitive permutation 2-group with a transposition. Then there exists $C_G > 0$ such that

$$\lim_{X\to\infty} \frac{\sum_{K\in\mathcal{F}_G(X)} h_3(K)}{\sum_{K\in\mathcal{F}_G(X)} 1} = C_G.$$

Thank you !