Pointwise Bound for ℓ-torsion in Class Groups

Jiuya Wang
Duke University

Harvard University, Sept 30, 2019

Class Group Problem

Question

Q : How large is class group ? ℓ-torsion of class group ?

$\mathcal{A}_F[\ell] := \{\alpha \in \mathcal{A}_F \mid \ell \cdot \alpha = 0\}$

Theorem (Brauer-Siegel, Minkowski)

Given an arbitrary extension $F/\mathbb{Q}$ with degree d, we have

$$|\mathrm{Cl}_F| = O_{\epsilon,d}(\mathrm{Disc}(F)^{1/2+\epsilon}).$$

What do we expect ?

ℓ-torsion Conjecture

Conjecture (Cohen-Lenstra Heuristics)

Given an odd prime ℓ and $k > 0$. We have for quadratic fields

$$\lim_{X\to\infty} \frac{\sum_{F,0<\mathrm{Disc}_F<X} |\mathrm{Cl}_F[\ell]|^k}{\sum_{F,0<\mathrm{Disc}_F<X} 1} = C_{k,\ell}.$$

Certain finite

[PTBW, 2018]

Conjecture (ℓ-torsion Conjecture)

Given a transitive permutation subgroup $G \subset S_n$ and a prime ℓ. Then for every G-extension $F/\mathbb{Q}$,

$$|\mathrm{Cl}_F[\ell]| = O_\epsilon(\mathrm{Disc}(F)^\epsilon).$$

Conclusion : ℓ- torsion conj is at a coarser scale.

A Clear Dichotomy on ℓ

Theorem (Gauss)

For every quadratic extension $F/\mathbb{Q}$, we have

$$|\mathrm{Cl}_F[2]| = O_\epsilon(\mathrm{Disc}(F)^\epsilon).$$

Reason : Genus Theory. $rk_2 Cl_F[2] = \omega(\mathrm{Disc}(F)) - 1$

A Clear Dichotomy on ℓ

Theorem (Gauss)

For every quadratic extension $F/\mathbb{Q}$, we have

$$|\mathrm{Cl}_F[2]| = O_\epsilon(\mathrm{Disc}(F)^\epsilon).$$

Reason : Genus Theory

Theorem (Klüners-W.,2020)

For every ℓ-extension $F/\mathbb{Q}$, we have

$\mathrm{Gal}(\widetilde{F}/\mathbb{Q})$ is ℓ-grp

$$|\mathrm{Cl}_F[\ell]| = O_\epsilon(\mathrm{Disc}(F)^\epsilon).$$

Upper Bound Type Conjectures

There are also other upper bound conjectures in arithmetic statistics :

- number of number fields with fixed discriminant (Discriminant multiplicity conjecture) ✓
- number of number fields with bounded discriminant (Weak Malle's conjecture) ✓
- number of elliptic curves with fixed conductor
- rank of $Jac(C)$ for hyper-elliptic curves C

Consequence : both conjectures hold for nilpotent extensions.

Modern Result : Small ℓ

Status : when there is no genus theory, we are still trying to break the trivial bound. $|Cl_F[\ell]| \leq |Cl_F| = O_\varepsilon(D_F^{1/2+\varepsilon})$

Definition

We will say a bound in the form of $|\mathrm{Cl}_F[\ell]| = O(\mathrm{Disc}(F)^{1/2-\delta})$ for any $\delta > 0$ a *non-trivial* upper bound on $\mathrm{Cl}_F[\ell]$.

Modern Result : Small ℓ

Status : when there is no genus theory, we are still trying to break the trivial bound.

Definition

We will say a bound in the form of $|\mathrm{Cl}_F[\ell]| = O(\mathrm{Disc}(F)^{1/2-\delta})$ for any $\delta > 0$ a *non-trivial* upper bound on $\mathrm{Cl}_F[\ell]$.

Theorem (Pierce 05, Helfgott-Venkatesh 06)

The size of $\mathrm{Cl}_F[3]$ *for quadratic fields over* $\mathbb{Q}$ *are non-trivially bounded*

Modern Result : Small ℓ

Theorem (Ellenberg-Venkatesh 07)

The size of $\mathrm{Cl}_F[3]$ *for number fields over* $\mathbb{Q}$ *with* $\deg \leq 4$ *are non-trivially bounded.*

For $\ell = 2$, we have a much more general result.

Theorem (BSTTTZ, 17)

Given arbitrary $G \subset S_n$. *For every* G*-extension* $F/\mathbb{Q}$, *we have*

$$|\mathrm{Cl}_F[2]| \leq O_{\epsilon,n}(\mathrm{Disc}(F)^{1/2-1/2n+\epsilon}).$$

Modern Result : Large ℓ

For general $\ell > 3$, there are more recent results based on the following critical lemma in the work of Ellenberg-Venkatesh.

Lemma (Ellenberg-Venkatesh,07)

Given $L/\mathbb{Q}$, a prime ℓ, and $0 < \theta < \frac{1}{2\ell(d-1)}$, denote

as ℓ becomes large.

$$M := \pi(\mathrm{Disc}(L)^{\theta}; L, e),$$

the range is arbitrarily short.

then

$$|\mathrm{Cl}_L[\ell]| \leq O_{\epsilon}\left(\frac{\mathrm{Disc}(L)^{1/2+\epsilon}}{M}\right). \quad (1)$$

Difficulty : θ is too small !

If we are allowed to assume GRH,

Theorem (Lagarias-Odlyzko, 75)

Given a Galois extension L/K with Galois group G. Assuming GRH, then for every $x \geq 2$, we have

$$\left|\pi(x; L/K, e) - \frac{1}{|G|}\mathrm{Li}(x)\right| = O_{[L:\mathbb{Q}]}(x^{1/2}\ln(\mathrm{Disc}(L)x)).$$

then we get

Theorem (Ellenberg-Venkatesh, 2007)

Assume GRH for Artin L-function. Then for every $\ell > 0$, and every $G \subset S_n$, there exists $\delta(\ell, G) = 1/2\ell(d-1)$ such that

$$|\mathrm{Cl}_F[\ell]| = O_\epsilon(\mathrm{Disc}(F)^{1/2-\delta(\ell,G)+\epsilon}).$$

Modern Result : Unconditional

If we cannot hope to give good lower bound on enumerating small split prime ideals for one single number field, we can at least hope to say that *on average* the expected lower bound on small split prime ideals holds for most number fields.

Theorem (Ellenberg-Pierce-Wood, 2016)

For arbitrary ℓ, there exists $\delta(\ell) > 0$ such that for all non-D_4 number fields with $\deg \leq \frac{4}{5}$, *we have*

$$\sum_{\mathrm{Disc}(F)<X} |\mathrm{Cl}_F[\ell]| = O(X^{3/2-\delta(\ell)}).$$

- good for many applications.

Modern Result : Unconditional

If we cannot hope to prove GRH for a single L-function, we can at least say altogether *on average* there aren't too many zeroes for a family of L-functions.

Theorem (Pierce-Turnage-Butterbaug-Wood, 2018)

For some Galois group G with ramification constraints, almost all G-extensions L satisfies

$$\left|\pi(x; L, e) - \frac{1}{|G|}\frac{x}{\log x}\right| = O\left(\frac{x}{\log^A x}\right),$$

for some $A \geq 2$.

There are also other results along this line : Widmer (2018), An (2018), Frei-Widmer (2018, 2019), Thorner-Zaman (2019),...

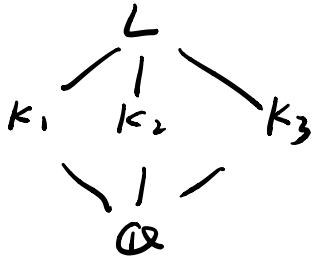
Critical Input: Enumerating Nubes Fields.

Motivation

When we look at number fields $L/\mathbb{Q}$ containing many subfields

- Insufficiency of enumerating number fields as an input.
- No need to ask the whole Dedekind-zeta function to be zero-free.

eg. $G = C_2 \times C_2$



- $\zeta_L / \zeta = \zeta_{K_1}/\zeta \cdot \zeta_{K_2}/\zeta \cdot \zeta_{K_3}/\zeta$.
- $Cl_L[\ell] = Cl_{K_1}[\ell] \times Cl_{K_2}[\ell] \times Cl_{K_3}[\ell]$.

Galois module structure

Lemma

Given an elementary abelian group $A = (\mathbb{Z}/p\mathbb{Z})^r$ with $r > 1$ and a prime ℓ with $(\ell, p) = 1$. For arbitrary A-extension L/k, we have

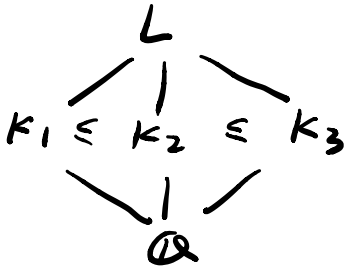
$$|\,\mathrm{Cl}_{L/k}[\ell]| = \prod_{K_i/k} |\,\mathrm{Cl}_{K_i/k}[\ell]|,$$

$$\mathrm{Disc}(L/k) = \prod_{K_i/k} \mathrm{Disc}(K_i/k),$$

where K_i/k ranges over all subfields of L with $[K_i : k] = p$.

Elementary Abelian Extensions

$G = C_2 \times C_2$

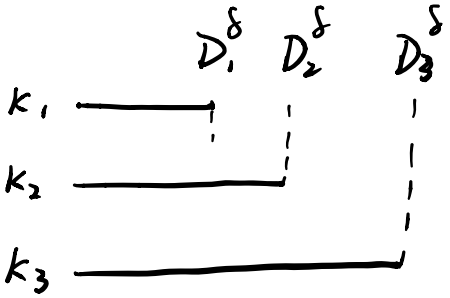


$K_i = \mathbb{Q}(\sqrt{D_i})$ $D_i > 0$

Use symmetries :

- $Disc(K_1) = QR$ => only K_1 can be small.
  $Disc(K_2) = RS$
  $Disc(K_3) = QS$
- $\left(\frac{P}{D_1}\right)\cdot\left(\frac{P}{D_2}\right)\cdot\left(\frac{P}{D_3}\right) = 1$ => primes has to split
- $Cl_L[\ell] = Cl_{K_1}[\ell] \times Cl_{K_2}[\ell] \times Cl_{K_3}[\ell]$
  $Disc(L) = \prod_i Disc(K_i)$

A Sketch of Proof



If K_1 is big, then apply pigeon hole principle to D_1^θ.

If K_1 is small, then construct many inert primes for K_1 up to D_2^δ.

Existence of Large Primes

Theorem (Maynard 13, Zaman 17)

Given L/k a Galois extension of number fields with $[L:\mathbb{Q}] = d$. There exists absolute, effective constants $\gamma = \gamma(k, G) > 2$, $\beta = \beta(k, G) > 2$, $D_0 = D_0(k) > 0$ and $C = C(k) > 0$ such that if $\mathrm{Disc}(L/k) \geq D_0$, then for $x \geq \mathrm{Disc}(L/k)^\beta$, we have

$$\pi(x; L/k, \mathcal{C}) \geq C_k \frac{1}{\mathrm{Disc}(L/k)^\gamma} \cdot \frac{|\mathcal{C}|}{|G|} \cdot \frac{x}{\ln x}.$$

Theorem (Brun-Titchmarsh,73)

For $x > q$, we have

$$\pi(x; q, a) \leq \left(\frac{2}{1 - \ln q / \ln x}\right) \frac{x}{\phi(q) \ln x}.$$

Induction : High Rank

Corollary

Given an elementary abelian group $A = (\mathbb{Z}/p\mathbb{Z})^r$ with $r > 2$ and a prime ℓ such that $(\ell, p) = 1$, then we have for arbitrary A-extension L/k,

$$\begin{aligned} |\mathrm{Cl}_{L/k}[\ell]| &= \prod_{M_j/k} |\mathrm{Cl}_{M_j/k}[\ell]|^{(p-1)/(p^{r-1}-1)} \\ &= \prod_{F_s/k} |\mathrm{Cl}_{F_s/k}[\ell]|^{(p-1)/(p^{r+1-t}-1)}. \end{aligned} \tag{2}$$

where M_j/k ranges over all subfields of L with $[M_j : k] = p^2$, and F_s/k ranges all subfields of L with $[F_s : k] = p^t$.

Main Theorem

Theorem (W. 2020)

Given $A = (\mathbb{Z}/p\mathbb{Z})^r$ with arbitrary prime number p and $r > 1$ and a prime ℓ. Then for every A-extension $L/\mathbb{Q}$, there exists $\delta(\ell, p) > 0$ such that

$$|\mathrm{Cl}_L[\ell]| = O_\epsilon(\mathrm{Disc}(L)^{1/2-\delta(\ell,p)+\epsilon}).$$

Remark :

- Pointwise ✓
- Insensitive to base field ✓
- Break the GRH bound when r is large ✓

How to generalize

What is at the heart of the argument ?

- Galois module structure
- Galois structure !!

Heart of the Argument : we can force the existence of small split primes in K_3/K_2 via constructing large inert primes in K_1.

Forcing Extensions

To generalize this idea *vertically*, we define the following type of group extensions.

Definition (Forcing Extension)

We say that a group extension $(\tilde{G}, \pi)$ of G

$$0 \to H \to \tilde{G} \to G \to 0$$

is *forcing* if there exists a conjugacy class $\mathcal{C} \subset G$ such that for every element $c \in \mathcal{C}$, all elements in $\pi^{-1}(c) \subset \tilde{G}$ has the same order with $c \in G$. We will also say that $(\tilde{G}, \pi)$ is *forcing with respect to* $\mathcal{C}$.

Inductive Argument

For an arbitrary integer $\ell > 1$, we denote $\mathcal{G}(\ell)$ to be the set of permutation Galois groups G where $|\mathrm{Cl}_F[\ell]|$ is non-trivially bounded for every G-extension F/k.

Lemma (W. 2020)

Suppose the regular representation of G is in $\mathcal{G}(\ell)$. If a group extension $(\tilde{G}, \pi)$ of G

$$0 \to H \to \tilde{G} \xrightarrow{\pi} G \to 0$$

is a forcing extension with respect to $\mathcal{C}$, then the regular representation $\tilde{G}$ is also in $\mathcal{G}_k(\ell)$.

p-Group Theory

Lemma (W. 2020)

Every non-cyclic and non-quaternion p-group G has a decreasing sequence of normal subgroups N_i

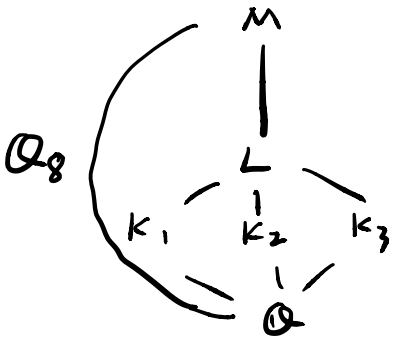
$$G \supset \Phi(G) = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_m = e,$$

where for every $0 \leq i < m$:
1) $[N_i : N_{i+1}] = p$;
2) $(G/N_{i+1}, \pi)$ is a forcing extension of G/N_i where $\pi : G/N_{i+1} \to G/N_i$.

Quaternion Groups

From the point of view of group theory, the generalized quaternion group is interesting :

- It is the only non-cyclic p-groups where all abelian subgroups are cyclic.
- It has trivial Schur multiplier.



Theorem (W. 2020)

The regular representation for every non-cyclic and non-quaternion p-group G is in $\mathcal{G}(\ell)$. More generally, if the Sylow-p subgroup G_p for a nilpotent group G is non-cyclic and non-quaternion for every $p||G|$, then the regular representation of G is in $\mathcal{G}(\ell)$.

(Bhargava – Shankar – Taniguchi – Thorne – Tsimerman – Zhao)

	G \ ℓ	$\ell = 2$	$\ell = 3$	$\ell = 5$	...
(GRH)	(Ellenberg – Venkatesh) all G				
	(Ellenberg – Venkatesh) $d \leq 4$				
(O.A)	(Ellenberg – Pierce – Wood) (Widmer). $d \leq 5$ (non D_4)				
(O.A)	(Pierce – Turnage – Buttcane – Wood). (Zaman – Thorne) S_n, A_n, D_n, w/ ram conditions				
	W. most p-extensions and nilpotent extensions related				

Thank you !