Non-trivial bounds on 2, 3, 4, and 5-torsion in class groups of number fields, conditional on standard $L$-function conjectures

Arul Shankar and Jacob Tsimerman

August 8, 2023

Abstract

We prove new conditional bounds on the $m$-torsion subgroups of class groups of number fields of any fixed degree, for $m = 2, 3, 4,$ and $5$. Our methods first recast the problem in the language of class groups of Galois modules, which allows us to relate these torsion subgroups to Selmer groups of elliptic curves. We then obtain a global estimate using the refined BSD conjecture, in a similar way to how one normally uses the Brauer–Siegel bound.

Our methods are potentially very general, but rely on the existence of motives with very special $\mathbb{Z}/m\mathbb{Z}$-cohomology. In particular, the restriction to $m \leq 5$ stems from needing an elliptic curve over $\mathbb{Q}$ with $m$-torsion subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mu_m$.

1 Introduction

History and main results

Let $n, m \geq 2$ be fixed integers. For any number field $K$ of degree $n$, it is conjectured that the size $h_m(K)$ of the $m$-torsion subgroup of the class group of $K$ satisfies the bound $h_m(K) = O_{n,m}(|\text{Disc}(K)|^{\epsilon})$ for every $\epsilon > 0$. This conjecture is currently known only for $n = m = 2$ (using Gauss’s genus theory). For other degrees and primes, the best that is known in general is the bound

$$h_m(K) = O_{n,\epsilon}(|\text{Disc}(K)|^{1/2+\epsilon}),$$

which follows from the Brauer–Siegel theorem bounding the size $h(K)$ of the entire class group, and applying the trivial inequality $h_m(K) \leq h(K)$. It has become a problem of much interest to obtain any improvement on the trivial bound \(^4\) for any pair $(n, m) \neq (2, 2)$.

The first such result was obtained independently by Pierce \(^1\) and Helfgott–Venkatesh \(^2\), who consider the case $n = 2$ and $m = 3$, and prove the bounds $O_{\epsilon}(|\text{Disc}(K)|^{27/56+\epsilon})$ and $O_{\epsilon}(|\text{Disc}(K)|^{0.44178-\epsilon})$, respectively. Subsequently, these bounds were improved to $O_{\epsilon}(|\text{Disc}(K)|^{1/3+\epsilon})$ by work of Ellenberg and Venkatesh \(^3\). In this work, they also achieve the bound $O_{\epsilon}(|\text{Disc}(K)|^{1/3+\epsilon})$ for the cases $(n, m) = (3, 3)$ and $(4, 3)$. Recent work of Bhargava, Taniguchi, Thorne, Zhao and the two authors \(^2\) obtain power saving bounds $O(|\text{Disc}(K)|^{1/2-1/(2n)+\epsilon})$ for the case $m = 2$ for all degrees $n > 2$. Further unconditional results are also known when the number fields $K$ are constrained by having a fixed Galois group: in the work of Wang \(^4\), Kluners and Wang \(^5\), and Wang \(^6\), power saving bounds are respectively obtained for $p$-torsion in the class groups of $K$, where $K$ has Galois group $(\mathbb{Z}/q\mathbb{Z})^r$ (here $q$ is prime and $r > 1$), where the Galois group of $K$ is a $p$-group, and where the Galois group of $K$ is a nilpotent group $G$ such that every Sylow subgroup of $G$ is non-cyclic and non- quaternion. Additionally, conditional on the generalized Riemann hypothesis, Ellenberg and Venkatesh prove a bound of $O(|\text{Disc}(K)|^{\frac{r^2}{2} + \frac{m(n-m)+\epsilon}{2m(n-m)^{1/2}}})$ for all pairs $(n, m)$.

The purpose of this paper is to introduce a new method for obtaining such bounds, albeit a conditional one at the moment. Our main result is the following.

**Theorem 1** Let $n > 1$ be a fixed integer, and let $m = 2, 3, 4,$ or $5$. Assume the Hasse–Weil conjecture, the refined Birch and Swinnerton-Dyer conjecture, and the generalized Riemann hypothesis for $L$-functions of elliptic curves over degree-$n$ number fields. Then $h_m(K) = O_{n,\epsilon}(D^{1/2+\epsilon})$ for any degree-$n$ number field $K$. 
In the case of quadratic fields, we can get a non-trivial result without assuming either the Hasse–Weil conjecture or the generalized Riemann hypothesis:

**Theorem 2** Let $m = 4$ or $5$. Assume the refined Birch and Swinnerton-Dyer conjecture for elliptic curves over $\mathbb{Q}$. Then $h_m(\mathbb{Q}(\sqrt{D})) = O(\frac{1}{2} - \delta)$ where $\frac{1}{2} - \delta$ is the best subconvex bound we have for $L$-functions of elliptic curves over $\mathbb{Q}$.

**Remark 3** We make the following three observations regarding Theorem 1 and its proof.

(a) To our knowledge, this is the first (even conditional) result which gives pointwise bounds, where the quality of the exponent does not degrade with the degree $n$ of the number field.

(b) To obtain the conclusion of Theorem 1, we need to assume something weaker than the three conjectures for all elliptic curves $E/K$. In fact, we only use base changes of a single elliptic curve.

(c) If, for a fixed elliptic curve $E/\mathbb{Q}$, we had a way of bounding the rank of $E/K$ by $o(\log |\text{Disc}(K)|)$ unconditionally, we would not need to assume the generalized Riemann Hypothesis for the $L$-function of $E/K$. Assuming the Lindelöf conjecture for this $L$-function would be sufficient. Moreover, any subconvex estimate on the central value of this $L$-function would also imply a power saving bound on the torsion in the class group.

**Method of proof**

Our perspective is as follows.

1. First, for an integer $m$, we express the group $\text{Cl}(K)[m]$ as an unramified cohomology group of a finite Galois module $M$. In fact, $M$ is simply $\mathbb{Z}/m\mathbb{Z}[\text{Hom}(K, \bar{\mathbb{Q}})]$. We denote this unramified cohomology group by $\text{Cl}(M)$.

2. Our main idea (philosophically, and somewhat imprecisely) is to find other ‘motives’ $X$ whose mod $m$-reduction is (essentially) isomorphic to a power of $M$. Then we may hope to reinterpret $\text{Cl}(M)$ as the $m$-torsion of a motivic class group $\text{Cl}(X)$. There should be a global class number formula for $\text{Cl}(X)$ with a trivial bound that one can use to bound $\text{Cl}(M)$. In a sense, we are obtaining better “trivial bounds” for $\text{Cl}(M)$ by embedding $M$ into different motives.

3. Concretely, we find an elliptic curve $E$ over $\mathbb{Q}$ such that $E[m]$ is isomorphic to $\mu_m \oplus (\mathbb{Z}/m\mathbb{Z})$ as Galois modules over $\mathbb{Q}$. It is known that such elliptic curves only exist when $m$ is 2, 3, 4, and 5, hence our results are limited to these four values of $m$. Our motive is essentially the Abelian variety $A = \text{Res}_{K/\mathbb{Q}}E_K$ and its class group corresponds to the Tate-Shafarevich group. The torsion group scheme $A[m]$ is isomorphic to $\mathbb{Z} \oplus \mu_m$, and we show that $\text{Cl}(M)$ and $\text{Cl}(\mathbb{Z} \oplus \mu_m)$ are approximately the same size (in fact they are dual to each other up to small error).

4. The Refined BSD conjecture plays the role of the class number formula which allows us a method for computing the size of $\text{III}_A$, assuming we have control on the rank of $A$ and the size of the central value of the $L$-function. This is where the generalized Riemann hypothesis enters. We then use GRH to provide an upper bound for $\text{III}_A$. This in turn provides a trivial upper bound for $\text{III}_A[m]$, which we show is essentially the same size as $\text{Cl}(A[m])$ (once the size of the rank has been controlled). Combining these observations gives an upper bound for $\text{Cl}(M)$.

In fact, we find it easier to work with $E/K$ directly and not form the Weil-restriction down to $\mathbb{Q}$, but this is a minor point done for technical convenience.

**Acknowledgements**

We are happy to thank Ashay Burungale, Jordan Ellenberg, Ananth Shankar, Joe Silverman, and Tonghai Yang for interesting comments and corrections on a previous version of this paper.

1The best such bound the authors are aware of is $\delta = \frac{25}{256}$ (see [1]).
2 Estimating the terms in the refined BSD conjecture

Let $E$ be an elliptic curve over $\mathbb{Q}$, and let $K$ be a degree-$n$ number field. Let $L(E/K, s)$ denote the Hasse–Weil $L$-function of $E$ over $K$, normalized so that the critical line is $\Re(s) = 1$. We denote the completed $L$-function of $E/K$ by $\Lambda(E/K, s)$:

$$\Lambda(E/K, s) := \text{Norm}_{K/\mathbb{Q}}(N_{E/K})\Gamma(K)^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(E/K, s),$$

where $N_{E/K}$ is the conductor ideal of $E$ over $K$ and $\Gamma_K(s) := ((2\pi)^{-s}\Gamma(s))^n$. We begin by recalling three standard conjectures regarding $E/K$ and its $L$-function. First, the Hasse–Weil conjecture (HWC) for $E/K$ is the following:

**Conjecture 2.1** The function $L(E/K, s)$ has an analytic continuation to the entire complex plane, and satisfies the function equation

$$\Lambda(E/K, s) = w(E/K)\Lambda(E/K, 2 - s),$$

where $w(E/K)$ denotes the root number of $E/K$.

Denote the algebraic rank of $E/K$ by $r_{E/K}$. The refined Birch and Swinnerton-Dyer (BSD) conjecture for $E/K$ is the following:

**Conjecture 2.2** The algebraic rank $r_{E/K}$ is equal to the order of vanishing of $L(E/K, s)$ at $s = 1$. Moreover, the leading term of the Taylor series of $L(E/K, s)$ at $s = 1$ is given by

$$\lim_{s \to 1} \frac{L(E/K, s)}{(s-1)^{r_{E/K}}} = |\text{Disc}(K)|^{-1/2} \cdot \#\Sha(E/K) \cdot R_{E/K} \cdot \Omega_{E/K} C_{E/K} \frac{C_{E/K}}{\#E(K)^2_{\text{tor}}},$$

Above, $\text{Disc}(K)$ denotes the discriminant of $K$, $\Sha(E/K)$ is the Tate–Shafarevich group of $E$ over $K$, $R_{E/K}$ is the regulator of $E$ over $K$, $\Omega_{E/K} := \Omega_{E,K}^\prime \Omega_{E,K}^\prime$ is the product of the two periods of $E$ raised to the number of real and complex embeddings of $K$, respectively, and $C_{E/K}$ is given by

$$C_{E/K} := \prod_v c_v(E/K) \left| \frac{\Delta_{E,v,\min}}{\Delta_{E,v}} \right|_{v}^{\frac{1}{2}},$$

where the product is over all finite places $v$ of $K$, and where $\Delta_{E,v,\min}$ denotes the discriminant of a minimal model for $E$ over $K_v$.

Finally, we have the Grand Riemann Hypothesis (GRH) for the $L$-function of $E/K$.

**Conjecture 2.3** The nontrivial zeroes of $L(E/K, s)$ lie on the line $\Re(s) = 1$.

In the remainder of the section, we obtain bounds on the rank $r_{E/K}$ of $E/K$ and the size of the Tate–Shafarevich group $\Sha(E/K)$ conditional on the above three conjectures on $E/K$. Our bounds are in the setting where $E$ and the degree $n$ of the number field $K$ are fixed, while $K$ is varying.

We begin with the following lemma.

**Lemma 2.4** We have

$$1 \ll_{n,E} \frac{\Omega_{E/K} C_{E/K}}{\#E(K)^2_{\text{tor}}} \ll_{n,E} 1.$$

**Proof:** The quantity $\Omega_{E/K}$ depends only on $E$ and the number of real and complex embeddings of $K$. By Merel’s generalization [14] of Mazur’s theorem [13], it follows that we have $\#E(K)^2_{\text{tor}} \ll_{E} 1$. We also have the inequalities

$$1 \ll \prod_v \left| \frac{\Delta_{E,v,\min}}{\Delta_{E}} \right|_{v} \ll_{n,E} 1, \quad 1 \ll \prod_v c_v(E/K) \ll_{n,E} 1,$$

where the first two inequalities are immediate, and the second two follow from an argument identical to the proof of [16, Lemma 6.2.1]. \(\square\)

Next, we have the following conditional bounds on the rank of $E/K$ from [8, Proposition 5.21].
Lemma 2.5 Assume that $E/K$ satisfies the HWC and the BSD conjecture, and that $L(E/K, s)$ satisfies GRH. Then we have
\[ r_{E/K} \ll_{n,E} \frac{\log |\text{Disc}(K)|}{\log \log |\text{Disc}(K)|}. \]

Next, we obtain a lower bound on the regulator depending on the rank of $E/K$:

Lemma 2.6 With notation as above, we have
\[ R_{E/K} \gg_{n,E} \left( \frac{\log |\text{Disc}(K)|}{r_{E/K}} \right)^{r_{E/K}}. \]

Proof: Let $P = (x, y) \in E(K)$ be a rational point. Let $F = \mathbb{Q}(x, y)$ be the subfield of $K$ generated by $x$ and $y$. We know that the canonical height $h(P)$ of $P$ is within $O_E(1)$ of the Weil height of $P$ which is simply the logarithmic height of $x \in \mathbb{Q}$. Since $x$ generates $F$, it follows that we have $h(P) \gg_E \log |\text{Disc}F|$. Moreover, by Lemma 2.5, we know that the rank of $E$ over $F$ is $\ll_{n,E} \log |\text{Disc}(F)|$. The lemma now follows from Minkowski’s second theorem. \qed

Remark 2.7 We note that sophisticated lower bounds for the canonical heights of nontorsion points in elliptic curves $E/K$ are proven by Silverman [19] and Hindry–Silverman [7]. However, those results are proven in the setting where $K$ is fixed and $E$ is varying, while we need bounds in the setting where $E$ is fixed and $K$ is varying.

The conductor of $L(E/K, s)$ is $\text{Disc}(K)^2 \text{Norm}_{K/Q}(A(E/K)) \ll E \text{Disc}(K)^2$. This yields the “convex” bound $|L(E/K, s)| \ll_{E,\epsilon} |\text{Disc}(K)|^{1/2+|s|+\epsilon}$, for complex numbers $s$ sufficiently close to 1. In our next result, we bound the leading Taylor coefficient of the $L$-function $L(E/K, s)$, assuming a rank bound on $E/K$ and a subconvex bound on $|L(E/K, s)|$.

Lemma 2.8 Assume that we have $|L(E/K, s)| \ll_{E,\epsilon} |\text{Disc}(K)|^{1/2+|s|} |^{1/2-\eta+\epsilon}$ for some $\eta > 0$, and that the rank of $E$ over $K$ is bounded by $r_{E/K} \ll_{E,\epsilon} \log |\text{Disc}(K)|/\log \log |\text{Disc}(K)|$. Then we have
\[ \lim_{s \to 1} \frac{L(E/K, s)}{(s-1)^{r_{E/K}}} \ll_{E,\epsilon} |\text{Disc}(K)|^{1/2-\eta+\epsilon}. \]

Proof: Denote $r_{E/K}$ by $r$ and note that the result is immediate when $r = 0$. When $r \geq 1$, we write
\[ \lim_{s \to 1} \frac{L(E/K, s)}{(s-1)^{r}} = L^{(r)}(E/K, 1) = r! \cdot \text{Res}_{s=0} \frac{L(E/K, 1+s)}{s^{r+1}}. \]

Therefore, from the residue theorem, we have
\[ L^{(r)}(E/K, 1) = \frac{1}{2\pi i} \int_{|s|=\theta} \frac{L(E/K, 1+s)}{s^{r+1}} ds \]
for every $\theta > 0$. Taking $\theta = (\log \log \log |\text{Disc}(K)|)^{-1}$ and using the upper bound on $r$ yields
\[ L^{(r)}(E/K, 1) \ll_{E,\epsilon} |\text{Disc}(K)|^{1/2-\eta+\epsilon}, \]
as necessary. \qed

Finally, we combine 2.3 with Lemmas 2.4, 2.5, 2.6, and 2.8 to obtain the following conditional upper bound on the Tate–Shafarevich group $\text{III}_{E/K}$.

Proposition 2.9 Let $E$ be a fixed elliptic curve over $\mathbb{Q}$ and let $n \geq 2$ be a fixed integer. Let $K$ be a number field of degree $n$, and assume Conjectures (HWC), (BSD), and (GRH) for $E/K$ and $L(E/K, s)$. Then we have
\[ \#\text{III}_{E/K} \ll_{n,E,\epsilon} |D|^{1/2+\epsilon}. \]
3 Comparing torsion in $\text{Cl}(K)$ to torsion in $\text{III}_{E/K}$

3.1 Cohomology of finite Galois modules over number fields

Let $A$ be a finite Galois module over a field $F$, i.e., a finite abelian group $A$, along with an action of the absolute Galois group $G_F$ of $F$ on $A$. We let $H^i(F,A)$ denote the $i$'th cohomology group arising from this action. Now let $A$ be a finite Galois module over a local field $K_v$ (with residue field denoted $\mathbb{F}_v$). Let $I_v$ denote the inertia subgroup of $G_{K_v}$. We say that $A$ is unramified if $I_v$ acts trivially on $A$. When $A$ is unramified, there is a natural action of $G_{K_v}/I_p \cong G_{\mathbb{F}_v}$ on $A$, and we have an injection

$$H^1(\mathbb{F}_v, A) \hookrightarrow H^1(K_v, A).$$

Define the subgroup of unramified cohomology classes by

$$H^1_{ur}(K_v, A) := \ker(H^1(K_v, A) \rightarrow H^1(I_v, A)).$$

When $A$ is unramified, it follows from the inflation-restriction exact sequence that the subgroup of unramified cohomology classes is exactly given by the image of $H^1(\mathbb{F}_v, A)$ (see [15, Lemma 3.2]).

Next, let $A$ be a finite Galois module over a number field $K$. Let $v$ be a place of $K$. The absolute Galois group $G_{K_v}$ of $K_v$ naturally injects into $G_K$, yielding natural maps $H^1(K, A) \rightarrow H^1(K_v, A)$. When $v$ is a finite place, we say that $A$ is unramified at $v$ if $A$ is unramified as a $K_v$-Galois module. We define the class group $\text{Cl}(A)$ of $A$ to be the set of elements $\sigma \in H^1(K, A)$ such that for every $v$ at which $A$ is unramified, the image of $\sigma$ in $H^1(K_v, A)$ is an unramified cohomology class. That is

$$\text{Cl}(A) := \ker\left( H^1(K, A) \rightarrow \prod_v H^1(K_v, A)/H^1_{ur}(K_v, A) \right),$$

where the product is over all finite places $v$ at which $A$ is unramified.

3.2 Selmer groups of elliptic curves

Let $E$ be an elliptic curve over a field $F$ and let $m$ be a positive integer. We have the exact sequence

$$0 \rightarrow E[m] \rightarrow E \rightarrow E \rightarrow 0,$$

of $G_F$-modules, where $E[m]$ is the $m$-torsion subgroup of $E$. This gives rise to the following exact sequence of Galois cohomology groups:

$$0 \rightarrow E(F)/mE(F) \rightarrow H^1(F, E[m]) \rightarrow H^1(F, E) \rightarrow 0. \quad (4)$$

We now specialize to the arithmetic case. Let $E$ be an elliptic curve over a number field $K$. We have the exact sequence $\text{(4)}$ for the fields $F = K$ and $F = K_v$ for all completions $K_v$ of $K$. The $m$-Selmer group $\text{Sel}_m(E)$ is then defined to be

$$\text{Sel}_m(E) := \ker\left( H^1(K, E[m]) \rightarrow \prod_v H^1(K_v, E) \right). \quad (5)$$

Above, the product is over all places $v$ of $K$, and the map $H^1(K, E[m]) \rightarrow H^1(K_v, E)$ is given by composing the map $H^1(K, E[m]) \rightarrow H^1(K_v, E[m])$ with the map $H^1(K_v, E[m]) \rightarrow H^1(K_v, E)$ of $\text{(4)}$.

Our next results compare the $m$-Selmer group of $E$ with the class group of the finite Galois module $E[m]$. We start with the following lemma.

**Lemma 3.1** Let $E$ be an elliptic curve over a number field $K$, and let $m > 1$ be an integer. Let $v$ be a place not dividing $m$ at which $E[m]$ is unramified and at which $E$ has good reduction. Then

$$\ker\left( H^1(K_v, E[m]) \rightarrow H^1(K_v, E) \right) = H^1_{ur}(K_v, E[m]).$$

That is, the image of a class $\sigma \in H^1(K_v, E[m])$ in $H^1(K_v, E)$ is soluble at $p$ if and only if it is unramified.
Proof: This is precisely the content of [3] Lemma 19.3. □

Proposition 3.2 Let $E$ be an elliptic curve over $K$ of degree $n$, and let $m > 1$. Let $s$ be the number of places of $K$ dividing $m\Delta(E)$. Then we have

$$\log\left(\frac{\#\text{Sel}_m(E)}{\#\text{Cl}(E[m])}\right) = O_{m,n}(s).$$

Proof: Both the groups $\text{Sel}_m(E)$ and $\text{Cl}(E[m])$ are subgroups of the Galois cohomology group $H^1(K, E[m])$. The Galois module $E[m]$ is unramified away from the prime dividing $m\Delta(E)$. It follows from Lemma 3.1 that the Selmer structures defining $\text{Sel}_m(E)$ and $\text{Cl}(E[m])$ differ at most at $s + n$ ‘bad’ local places (the $n$ coming from the infinite place of $K$). Thus $\log\left(\frac{\#\text{Sel}_m(E)}{\#\text{Cl}(E[m])}\right)$ is bounded by $\ln\prod_{v \text{ bad}} |H^1(K_v, E[m])|$. We are thus finished if we prove that $|H^1(K_v, E[m])| = O_{m,n}(1)$.

Let $N$ denote the subgroup of $G_{K_v}$ which fixes $E[m]$. Then by the inflation-restriction exact sequence, we have

$$|H^1(K_v, E[m])| \leq |H^1(G/N, E[m])| \cdot |H^1(N, E[m])| = |H^1(G/N, E[m])| \cdot |\text{Hom}(N, E[m])|.$$  

The first term in the second line of the above equation is $O_{m,n}(1)$ by virtue of having finitely many possibilities for $G/N$ and its action. On the other hand $|\text{Hom}(N, E[m])| = |N[m]|$ is bounded by $m$ times the number of degree $m$ extensions of $L = K_v^{\text{ur}}$ and hence by the number of degree $\leq d$ extensions of $Q_p$, where $d = mn \cdot \#\text{Aut} E[m]$. This is well-known to be uniformly bounded. □

3.3 Class groups of number fields

Let $K$ be a number field of degree $n$ over $Q$, and let $m > 1$ be a (fixed) integer. Class field theory provides a bijection between index-$m$ subgroups of $\text{Cl}(K)$ and degree-$m$ abelian extensions of $K$ which are unramified at every place. Let $v$ be a place of $K$. The set of degree-$m$ abelian extensions of $K$ (resp. $K_v$) is parametrized by $H^1(K, Z/mZ)$ (resp. $H^1(K_v, Z/mZ)$). Let $L$ be the extension of $K$ corresponding to $\sigma \in H^1(K, \mu_m)$. Then $L_v := L \otimes_K K_v$ corresponds to the image of $\sigma$ under the natural map $H^1(K, Z/mZ) \to H^1(K_v, Z/mZ)$. Furthermore, the extension $L_v$ of $K_v$ is unramified if and only if it corresponds to an unramified class in $H^1(K_v, Z/mZ)$. Therefore, the size of the $m$-torsion of the class group of $K$ is equal to the size of $H^1_{\text{ur}}(K, Z/mZ) = \text{Cl}(Z/mZ)$.

Meanwhile, we have the isomorphism $H^1(K, \mu_m) \cong K^\times/(K^\times)^m$ and, for a finite place $v$ of $K$ not dividing $m$, a class in $H^1(K, \mu_m)$ is unramified at $v$ if and only if it corresponds to an element in $K^\times/(K^\times)^m$ whose valuation at $v$ is divisible by $m$. Therefore, defining the group $A_{m,K}$ by

$$A_{m,K} \cong \left(\ker K^\times/(K^\times_m) \to \prod_v Z/mZ\right),$$

we see that $|\text{Cl}(\mu_m)|$ is within a factor of $O_{m,n}(1)$ of $|A_{m,K}|$.

There is a natural map $\phi : A_{m,K} \to \text{Cl}(K)[m]$ given by $\phi(\alpha) = (\alpha)^{\#m}$ which is surjective with kernel isomorphic to $U_K/U_K^m$, the $m$-cotorsion of the unit group of $K$. We thus obtain the following result:

Proposition 3.3 Let $K$ be a number field of degree $n$, and consider the $G_K$ modules $\mu_m, Z/mZ$. The group $\text{Cl}(Z/mZ)$ is isomorphic to the dual of $\text{Cl}(K)[m]$, and $\text{Cl}(\mu_m)$ has the same size as $\text{Cl}(K)[m]$ up to a factor of $O_{m,n}(1)$.

4 Proofs of Theorem 1 and 2

We begin with the following lemma.
Lemma 4.1 Let \( m \in \{2, 3, 4, 5\} \) be fixed. Then there exists an elliptic curve \( E/\mathbb{Q} \) such that we have the isomorphism

\[
E[m] \cong \mu_m \oplus \mathbb{Z}/m\mathbb{Z}
\]

as group schemes.

**Proof:** Since the modular curves \( \Gamma(m) \) have genus 0 for each \( m \in \{2, 3, 4, 5\} \), there do exist such curves. Below, we provide specific examples.

\[
m = 2. \quad E : y^2 = x^3 + x \\
m = 3. \quad E : y^2 + y = x^3 \\
m = 4. \quad E : y^2 + xy = x^3 - 4x - 1 \\
m = 5. \quad E : y^2 + y = x^3 - x^2 - 10x - 20
\]

These examples have been taken from the database LMFDB [10]. \( \square \)

Let \( m \) and \( E \) be as in the above lemma, and let \( K \) be a number field of degree \( n \). Denote the elliptic curve \( E \) over \( K \) by \( E_K \). We then have the isomorphism

\[
E_K[m] \cong \mu_m \oplus \mathbb{Z}/m\mathbb{Z}
\]

as group schemes. We next prove the following result.

**Proposition 4.2** The quantities \( \#\Sel_m(E_K) \) and \( #(\Cl(K)[m])^2 \) are within a factor of \( O_{\epsilon}(|\Disc(K)|^\epsilon) \) of each other.

**Proof:** By Proposition 3.2 we see that \( | \log \#\Cl(E_K[m]) - \log \#\Sel_m(E_K) | \) is bounded by \( O_{n,E}(1) \). By Proposition 3.3 we see that \( \#\Cl(\mathbb{Z}/m\mathbb{Z}) = \#\Cl(K)[m] \) and that \( | \log \#\Cl(\mu_m) - \log \#\Cl(K)[m] | \) is bounded by \( O_{n,m}(1) \). The result follows from the structure of \( E_K[m] \). \( \square \)

We are ready to prove the main results.

**Proof of Theorem 1** From the exact sequence

\[
0 \rightarrow \frac{E_K(K)}{mE_D(K)} \rightarrow \Sel_m(E_K) \rightarrow \Sha(E_K)[m] \rightarrow 0
\]

it follows that

\[
\#\Sel_m(E_K) = \#\left( \frac{E_K(K)}{mE_K(K)} \right) \cdot |\Sha(E_K)[m]|
\]

Our conditional rank bound from 2.5 implies that \( \#\left( \frac{E_K(K)}{mE_K(K)} \right) = O_{\epsilon}(|\Disc(K)|^\epsilon) \). Theorem 1 now follows immediately by combining Proposition 1.2 with the conditional bound on \( |\Sha(E_K)[m]| \) that was proved in Theorem 2.9 \( \square \)

**Proof of Theorem 2** let \( K = \mathbb{Q}(\sqrt{D}) \) be a quadratic field. Then the Weil restriction of \( E_K \) to \( \mathbb{Q} \) is isomorphic to the abelian surface \( E \oplus E_D \), where \( E_D \) denotes the twist of \( E \) by \( D \). Thus the Hasse–Weil conjecture for \( E_K \) is known by the modularity of \( E \) and \( E_D \).

Next, denote the Mordell-Weil rank of \( E_D \) by \( r_D \). Let \( \Sel_2(E_D) \) denote the 2-Selmer group of \( E_D \). From the exact sequence

\[
0 \rightarrow \frac{E_D(\mathbb{Q})}{2E_D(\mathbb{Q})} \rightarrow \Sel_2(E_D) \rightarrow \Sha(E_D)[2] \rightarrow 0
\]

we see that \( r_D \leq \log_2 \#\Sel(E_D) \). Since the field \( \mathbb{Q}(E_D(\mathbb{Q})[2]) \) is the same as \( \mathbb{Q}(E(\mathbb{Q})[2]) \), it follows from [3 Proposition 7.1] and [12 Proposition 9.8] that we have \( \log_2 \#\Sel(E_D) \ll \log_2 \#\Sel(E) + O(w_D) \), where \( w_D \) is the number of prime factors of \( D \). Therefore, we have the upper bounds

\[
r_{E/K} \ll E r_D \ll E \left( \frac{\log |D|}{\log \log |D|} \right)
\]  \( (6) \)
on the ranks of $E_D/\mathbb{Q}$ and $E_K$.

Assume that we have the subconvex bound $|L(E_D/\mathbb{Q}, s)| \ll_{E, \epsilon} |D|^{1/2+|s|-\delta+\epsilon}$ for some $\delta > 0$. This immediately implies the bound $|L(E/K, s)| \ll_{E, \epsilon} |\text{Disc}(K)|^{1/2}|s|^{-\delta+\epsilon}$. Theorem 2 now follows immediately from Lemma 2.8 by an argument identical to the proof of Theorem 1. 

\[ \square \]

References

[1] P. Autissier, M. Hindry, F. Pazuki, Regulators of Elliptic Curves, Int. Math. Res. Not. (IMRN), (2021), no. 7, 4976–4993.

[2] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao, Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. J. Amer. Math. Soc. 33 (2020), no. 4, 1087–1099.

[3] A. Brumer, K. Kramer, The rank of elliptic curves, Duke Math. J. 44 (1977), no. 4, 715–743.

[4] J. W. S. Cassels, Diophantine equations with special reference to elliptic curves, J. London Math. Soc. 41 (1966), 193–291.

[5] J. Ellenberg and A. Venkatesh, Reflection principles and bounds for class group torsion, Int. Math. Res. Not. IMRN 2007, no. 1.

[6] H. A. Helfgott and A. Venkatesh, Integral points on elliptic curves and 3-torsion in class groups, J. Amer. Math. Soc. 19 (2006), no. 3, 527–550.

[7] M. Hindry and J. Silverman, The canonical height and integral points on elliptic curves, Invent. Math. Vol. 93, 1988, 419–450.

[8] H. Iwaniec, and E. Kowalski, Analytic number theory, Vol. 53, American Mathematical Soc., 2021.

[9] J. Kl"uners and J. Wang, $\ell$-torsion Bounds for the Class Group of Number Fields with an $\ell$-group as Galois group, Proc. of the Amer. Math. Society, to appear.

[10] The LMFDB Collaboration, The L-functions and modular forms database, https://www.lmfdb.org 2023

[11] P. Maga, Subconvexity for twisted $L$-functions over number fields via shifted convolution sums, Acta Math. Hungary, 151 (2017), no. 1, 232–257.

[12] B. Mazur, Rational points of abelian varieties with values in towers of number fields, Invent. Math. 18 (1972), 183–266.

[13] B. Mazur, Modular curves and the Eisenstein ideal, With an appendix by Mazur and M. Rapoport, Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33–186.

[14] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Invent. Math. 124 (1996), no. 1-3, 437–449

[15] Milne, J. S. Arithmetic duality theorems, Second edition, BookSurge, LLC, Charleston, SC (2006), viii+339 pp.

[16] J. Park, B. Poonen, J. Voight, and M. Wood, A Heuristic for Boundedness of Ranks of Elliptic Curves, J. Eur. Math. Soc. (JEMS) 21 (2019), no. 9, 2859–2903.

[17] L. Pierce, A bound for the 3-part of class numbers of quadratic fields by means of the square sieve, Forum Math. 18 (2006), no. 4, 677–698.
[18] K. Rubin, Euler systems, *Annals of Mathematics Studies*, 147, Hermann Weyl Lectures, Princeton University Press, Princeton, NJ, 2000. xii+227 pp.

[19] J. Silverman, Lower bound for the canonical height on elliptic curves, *Duke Math. J.* 48 1981, 633-648

[20] J. Wang, Pointwise bound for ℓ-torsion in class groups: elementary abelian extensions, *J. Reine Angew. Math.* 773 (2021), 129–151.

[21] J. Wang, Pointwise Bound for ℓ-torsion in Class Groups II: Nilpotent Extensions, preprint.