

Reflection Principles and Bounds for Class Group Torsion

Jordan S. Ellenberg¹ and Akshay Venkatesh²

¹Department of Mathematics, University of Wisconsin, Madison and

²Courant Institute of Mathematical Sciences, New York University,
New York

Correspondence to be sent to: Akshay Venkatesh, Courant Institute of Mathematical Sciences, New York University, New York. e-mail: akshay.venkatesh@gmail.com

We introduce a new method to bound ℓ -torsion in class groups, combining analytic ideas with reflection principles. This gives, in particular, new bounds for the 3-torsion part of class groups in quadratic, cubic and quartic number fields, as well as bounds for certain families of higher degree fields and for higher ℓ . Conditionally on GRH, we obtain a nontrivial bound for ℓ -torsion in the class group of a general number field.

1 Introduction

The goal of the present article is to exhibit some bounds on the ℓ -part of the class group of a number field which improve on the trivial bound provided by the order of the entire class group. As such, they represent evidence towards a conjecture that the ℓ -part of the class group of a number field L of fixed degree grows more slowly than any power of the discriminant of L . Such conjectures have been suggested by Duke [1], for CM fields by Zhang [2, page 10] as the " ϵ -conjecture," and in a stronger form by Brumer and Silverman [3, "Question $CL(\ell, d)$ "]

Proposition 3.4 gives the bound $|D|^{1/3+\epsilon}$ for the 3-part of the class group of $\mathbb{Q}(\sqrt{-D})$. This improves the known bounds of [4] and [5] and has several corollaries (cf. [4, Section 4]). In combination with the techniques of [4] one obtains that there are at most $N^{0.169\dots}$ elliptic curves over \mathbb{Q} of conductor N . More directly, it implies that there are $\ll |D|^{1/3+\epsilon}$ cubic extensions of \mathbb{Q} with discriminant D .

Received July 18, 2006; Revised January 12, 2007; Accepted January 16, 2007
Communicated by Bjorn Poonen

See http://www.oxfordjournals.org/our_journals/imrn/ for proper citation instructions.

© The Author 2007. Published by Oxford University Press. All rights reserved. For permissions, please e-mail: journals.permissions@oxfordjournals.org.

Proposition 3.6 is our most general unconditional result on ℓ -torsion. A particular case of Proposition 3.6 is a nontrivial bound on the 3-torsion in even degree extensions of \mathbb{Q} with large Galois group; but it also has consequences for $\ell > 3$ and entails, e.g. a nontrivial bound for the 5-torsion part of the class group of any quadratic extension of $\mathbb{Q}(\sqrt{5})$. Finally, in Corollary 3.7 we apply these results to show a nontrivial bound on 3-torsion for cubic and quartic extensions of \mathbb{Q} .

The main results combine the use of noninert primes, an Arakelov version of the class group, and reflection principles of Scholz type. Roughly, the point is that small¹ noninert primes in a number field represent elements of the class group which tend not to satisfy any relation with small coefficients. (We are thinking of the class group “additively,” rather than “multiplicatively.”) Thus the existence of many such primes contributes significantly to the quotient of the class group by its ℓ -torsion, yielding the desired upper bounds. While it is known that unconditionally establishing the existence of such primes is very difficult, the GRH guarantees their existence, and this yields the conditional bound of Proposition 3.1. In order to remove the dependence on conjectures in some cases, we combine the argument on small primes with a weak version of the Scholz reflection principle. This yields Proposition 3.4 and Proposition 3.6. In this process, it is essential to deal with number fields with infinitely many units (even the bound for imaginary quadratic fields uses implicitly real quadratic fields, for instance); for such number fields, the above argument breaks down when implemented naively. Instead, we use an Arakelov version of the class group, in which the archimedean places do not play any distinguished role.

1.1 Sketch of proof for quadratic fields

Say D is negative and $D \equiv 1 \pmod{4}$. If \mathfrak{J} is an integral ideal of the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ with norm $\text{Norm}(\mathfrak{J}) < D$, then \mathfrak{J} cannot be principal unless it is the extension of an ideal of \mathbb{Q} ; for if we write $\mathfrak{J} = (x + y\sqrt{-D})$ and take norms, we see at once that y must vanish.

This easily implies that if:

- (1) p_1, \dots, p_r are distinct primes that split in $\mathbb{Q}(\sqrt{-D})$, and $e_i \in \mathbb{Z}$,
- (2) \mathfrak{p}_j is a prime ideal above p_j , and
- (3) $\prod_{j=1}^r \mathfrak{p}_j^{|e_j|} < D$

¹Small, in this context, will always mean “small relative to the discriminant of the number field.” More precisely, we shall require the norm of the prime to be less than a certain fixed small power of the discriminant.

then the product $\prod_i p_i^{e_i}$ cannot represent a trivial element of the class group. In other words, the p_i satisfy *no relation with small coefficients* (there is a small “piece” of the class group that tends to look free). Among other things, this means that some explicit subset of the p_i will represent distinct classes *modulo* ℓ -torsion, so given many such primes one gets an upper bound on the size of the ℓ -torsion part.

To adapt this idea to the real quadratic case $D > 0$ is not trivial, since there is no useful lower bound for the norm of a principal ideal. We fix this problem by using an “Arakelov” version of the class group that allows one to treat imaginary quadratic and real quadratic fields in a completely uniform way. This “Arakelov class group” is, in the quadratic field case, an extension of the usual class group by a circle; however, the “size” of the circle depends on the regulator. Using it we adapt the argument above to the general case.

With this in hand, we can explain the bound for quadratic fields. By Scholz’s theorem the 3-torsion in the class group of $\mathbb{Q}(\sqrt{-D})$ and $\mathbb{Q}(\sqrt{3D})$ have (up to a bounded factor) the same sizes. On the other hand, it is clear that *either* $\mathbb{Q}(\sqrt{-D})$ *or* $\mathbb{Q}(\sqrt{3D})$ must have many small split primes, because any prime of \mathbb{Q} which is inert in $\mathbb{Q}(\sqrt{-3})$ will split in one or the other field! These primes can be used to bound the size of the 3-torsion in the class group of one of the two fields – and by the reflection principle one thus has an unconditional bound for both fields. This yields a bound on order of $D^{1/3+\epsilon}$ for the size of the 3-torsion part of the class group of $\mathbb{Q}(\sqrt{-D})$.

1.2 Relation to existing work

As remarked, the following might be considered a “folk” conjecture. It is suggested in [1, Section 3]; it is explicitly conjectured in [2], and also is implied by a still stronger conjecture enunciated in [6, Conjecture 1.3].

Conjecture 1.1. (ϵ -conjecture for class group torsion). Let d, ℓ be fixed positive integers. Then the ℓ -torsion in the class group of any degree d field K has size $\ll_{\epsilon, \ell, d} (\text{disc } K)^\epsilon$.

There are many arithmetic settings in which one wishes to bound the size of a Galois cohomology group $H^1(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), M)$ for some finite abelian Galois module M ; usually the hard part of such a problem is control of the size of an ℓ -part of a class group. For instance, Conjecture 1.1 would imply strong bounds for the ranks of elliptic curves.

As to our methods: the idea of using small split primes in the context of class groups is an old one; in general, the difficulty in even proving that the class group must

be large for an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ is closely related to establishing the existence of enough small split primes.

In the context of torsion in class groups, this idea was already used (together with GRH) in the work of Boyd and Kisilevsky [7] on the exponent of the class group of imaginary quadratic fields; in the function field context, the same idea appears in an article of Madan and Madden [8]. (In the function field context, one knows the analogue of GRH and the results are thus unconditional). It came to our attention through the work of K. Soundararajan – implicitly in his article [9] and explicitly in private communication – and independently was suggested to us in a slightly different context by P. Michel.

As remarked, Proposition 3.4 improves on the results of Helfgott-Venkatesh [4] and Pierce [5] concerning the 3-part of quadratic class groups. (They proved, respectively, the bounds $\ll |D|^{0.441\dots}$ and $\ll |D|^{27/56}$, respectively, for general D ; in a separate article Pierce establishes the bound $\ll |D|^{5/12}$ for certain D that admit a divisor of specified size.) However, the methods of those two articles are, in certain ways, more robust than the method presented here. For instance, in the proof of Corollary 3.7 we implicitly make recourse to the methods of [4] to handle a case where our methods do not apply.

1.3 Notation

If K is a number field, we denote by Cl_K the ideal class group of K . If G is a locally compact abelian group and m an integer, we denote by $G[m]$ the m -torsion subgroup of G .

We use the analytic number theory notation $A \ll_B C$, for positive A, C , if there is a function $f(B)$ so that $A \leq f(B)C$ always. Similarly we define $A \gg_B C$. We write $A \asymp_B C$ if $C \ll_B A \ll_B C$.

If $K \subset L$ are global fields with rings of integers $\mathcal{O}_K \subset \mathcal{O}_L$, we say that a prime ideal \mathfrak{p}_K of \mathcal{O}_K *remains inert* in L if $\mathfrak{p}_K \mathcal{O}_L$ is a prime ideal of \mathcal{O}_L . In the case that $\mathfrak{p}_K \mathcal{O}_L$ is a prime ideal \mathfrak{p}_L , we say that \mathfrak{p}_L *is the extension of a prime ideal of K* . We denote by $\mathfrak{D}_{L/K}$ the relative discriminant of L/K ; it is an integral ideal of \mathcal{O}_K .

We denote by $\text{disc } K$ the absolute discriminant of the field K (i.e., $\text{disc } K \in \mathbb{N}$ is a generator for $\mathfrak{D}_{K/\mathbb{Q}}$).

2 Small noninert primes in the Arakelov class group

2.1 Introduction

In order to avoid problems arising from the group of units, we work consistently with an Arakelov class group, to be defined below.

Let K be a number field of degree d , and let I_K be the group of all fractional ideals of K . The usual ideal class group Cl_K is formed by taking the quotient I_K/K^\times . If K has more than one place at ∞ , this is in some sense an unnatural choice: for instance, if K were the function field of a curve C over \mathbb{F}_q , and R were the coordinate ring of an affine neighborhood of C , the ideal class group of R would be, not $\text{Pic}^0(C)$, but the quotient of $\text{Pic}(C)$ by the subgroup generated by the places in $C \setminus \text{Spec} R$. It is more natural to treat all places of K on the same footing, which means we have to consider Archimedean places as well.

The idea of doing this to give uniform approaches to the class group is well-known, although we do not know with whom it originates; see e.g. the exposition of Schoof [10].

2.2 Definition

To give a little motivation, we recall that the analytic class number formula gives an explicit expression for the product of the class number and the regulator of a number field K . The class number is the size of a group – the class group of K . The regulator is the *volume* of a group: the quotient of a Euclidean space by the unit lattice. It would be nice if we could “fit together” these two groups into a larger group, whose volume would equal the product of the class number and the regulator. This can indeed be done, and the “larger group” is the Arakelov class group.

Let K be a number field of degree d and set $K_\infty := K \otimes \mathbb{R}$. If M_K is the set of infinite places of K , i.e. equivalence classes of embeddings $\sigma : K \hookrightarrow \mathbb{C}$, then each $\sigma \in M_K$ extends to a homomorphism $\sigma : K \otimes \mathbb{R} \rightarrow \mathbb{C}$, whose image is either \mathbb{C} or \mathbb{R} according to whether σ is complex or real; we set $\deg(\sigma) = 2$ in the former case, and $\deg(\sigma) = 1$ in the latter. For $\sigma \in M_K$ we shall sometimes write $|x|_\sigma := |\sigma(x)|^{\deg(\sigma)}$.

There is a natural norm map $\text{Norm} : K_\infty \rightarrow \mathbb{R}_+$, given by

$$\text{Norm}(x) = \prod_{\sigma \in M_K} |x|_\sigma = \prod_{\sigma \in M_K} |\sigma(x)|^{\deg(\sigma)}.$$

Let K_∞^\times be the multiplicative group of K_∞ , and $K_\infty^{(1)} \subset K_\infty^\times$ the subgroup of elements of norm 1.

Let I_K be the (free abelian) group of fractional ideals of K , and write $\widetilde{\text{Div}}_K^0$ for the group $\{(x, J) \in K_\infty^\times \times I_K : \text{Norm}(x) = \text{Norm}(J)\}$. $\widetilde{\text{Div}}_K^0$ is a number-field analogue of the group of “divisor classes of degree 0.” Then K^\times is diagonally embedded in $\widetilde{\text{Div}}_K^0$; for $y \in K^\times$, we refer to $(y, (y)) \in \widetilde{\text{Div}}_K^0$ as the principal divisor associated to y .

We define² the *Arakelov class group* $\widetilde{\text{Cl}}_K$ to be $\widetilde{\text{Div}}_K^0/K^\times$. (Compare with the discussion of “modified Arakelov divisors” in [10].)

There is a natural projection map $\widetilde{\text{Cl}}_K \rightarrow \text{I}_K/K^\times = \text{Cl}_K$. This induces an exact sequence

$$K_\infty^{(1)}/\mathcal{O}_K^\times \rightarrow \widetilde{\text{Cl}}_K \rightarrow \text{Cl}_K \quad (2.1)$$

We now fix a measure on $K_\infty^{(1)}$. The choice is unimportant, so long as it done consistently. In fact, $K_\infty^{(1)}$ is the kernel of the map $K_\infty^\times \rightarrow \mathbb{R}^\times$ given by the norm, and K_∞^\times is the product of copies of \mathbb{C}^\times and \mathbb{R}^\times . We equip \mathbb{R}^\times with the Haar measure $\frac{dx}{x}$, and \mathbb{C}^\times with the measure $i\frac{dz \wedge d\bar{z}}{|z|^2}$. This induces a measure on $K_\infty^{(1)}$. Since (by means of the exact sequence above) $\widetilde{\text{Cl}}_K$ is locally isomorphic to $K_\infty^{(1)}$, we obtain also a measure on $\widetilde{\text{Cl}}_K$. Similarly $\widetilde{\text{Div}}_K^0$ is locally isomorphic to $K_\infty^{(1)}$, and we obtain also a measure on $\widetilde{\text{Div}}_K^0$. We denote both these measures by “vol”, for volume.

For instance, suppose K is a real quadratic field with regulator $R_K = |\log |\varepsilon||$. Here ε is the fundamental unit of K in either of its real embeddings. Then, the Arakelov class group is an extension of the usual ideal class group by the group $K_\infty^{(1)}/\mathcal{O}_K^*$. Now K_∞ is isomorphic to \mathbb{R}^2 , and $K_\infty^{(1)}$ is the hyperbola $xy = 1$ under this identification. The map $K_\infty^{(1)}/\mathcal{O}_K^* \rightarrow \mathbb{R}/R_K\mathbb{Z}$, given by $(x, 1/x) \mapsto \log |x|$, is a two-to-one covering. In particular, $K_\infty^{(1)}/\mathcal{O}_K^*$ has volume $2R_K$, and indeed it follows from definitions that this is true for arbitrary K . Therefore, the volume of $\widetilde{\text{Cl}}_K$ equals $2h_K R_K$ in this case, where h_K is the class number of K .

Lemma 2.1. With the normalization of measures above,

$$(\text{disc } K)^{1/2-\epsilon} \ll_{\epsilon, [K:\mathbb{Q}]} \text{vol}(\widetilde{\text{Cl}}_K) \ll_{\epsilon, [K:\mathbb{Q}]} (\text{disc } K)^{1/2+\epsilon}. \quad \square$$

Proof. Up to bounded constants (depending only on $[K:\mathbb{Q}]$) the volume of $\widetilde{\text{Cl}}_K$, with our normalizations, is equal to the product of the class number of K and the regulator at K . One then applies the Brauer-Siegel theorem.

There is a natural notion of *height* on $\widetilde{\text{Div}}_K^0$. Namely, for each (x, J) we define

$$H(x, J) = \prod_{\sigma \in \widetilde{M}_K} \max(|\sigma(x)|^{\deg(\sigma)}, 1) \cdot \prod_{\mathfrak{p}} \max(\text{Norm}(\mathfrak{p})^{-v_{\mathfrak{p}}(J)}, 1) \quad (2.2)$$

²An alternate definition, which we will not need here, is that the Arakelov class group consists of \mathcal{O}_K -stable lattices inside $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{R}$, up to the action of homotheties by \mathbb{R}^\times .

where the latter product is taken over primes \mathfrak{p} , and $v_{\mathfrak{p}}(J)$ is the power of \mathfrak{p} occurring in the prime factorization of J .

Then if $(y, (y))$ is the principal divisor associated to some $y \in K^\times$, the height of $(y, (y))$ is precisely the usual height $H(y)$ of y (considered as the point $(y : 1) \in \mathbb{P}^1(K)$).³

We will need the following lemma, which says that principal divisors cannot be of very low height unless they arise from subfields of K .

Lemma 2.2. Suppose K/K_0 is an extension of number fields of degree d and discriminant \mathfrak{D}_{K/K_0} and let λ be an element of K^\times such that $K_0(\lambda) = K$. Then $H(\lambda) \gg_{[K:\mathbb{Q}]}$ $\text{Norm}(\mathfrak{D}_{K/K_0})^{\frac{1}{2(d-1)}}$. \square

Proof. By embedding \mathbb{G}_m in \mathbb{P}^1 we may think of λ as a point $(\alpha : \beta)$ in $\mathbb{P}^1(K)$, with $\alpha, \beta \in \mathcal{O}_K$. Define

$$P = \prod_{i \neq j} (\alpha_i \beta_j - \beta_i \alpha_j) \quad (2.3)$$

where α_i, β_i run over the conjugates of α, β by the absolute Galois group of K_0 . Then $P \in \mathcal{O}_{K_0}$.

Any finite module M under \mathcal{O}_{K_0} is of the form $\bigoplus_j \mathcal{O}_{K_0}/\mathfrak{l}_j$, where \mathfrak{l}_j are certain integral ideals. The product $\prod_j \mathfrak{l}_j$ is an integral ideal which depends only on M . We refer to it as $\text{ind}(M)$.

Let L be the \mathcal{O}_{K_0} -span of $\alpha^{d-1}, \alpha^{d-2}\beta, \dots, \beta^{d-1}$. Let

$$L^* := \{\lambda \in K : \text{tr}_{K/K_0}(\lambda L) \subset \mathcal{O}_{K_0}\},$$

the dual of L w.r.t. the trace form. Then $L \subset L^*$ and $\text{ind}(L^*/L) = (P)$, the principal ideal generated by P – as follows by a direct computation.⁴

On the other hand, clearly $L \subset J := \langle \alpha, \beta \rangle^{d-1}$, the $(d-1)$ st power of the principal ideal generated by α, β . Moreover, $\text{ind}(J^*/J)$ equals $\text{Norm}_{K/K_0}(\langle \alpha, \beta \rangle)^{2d-2} \mathfrak{D}_{K/K_0}$. Consequently, (P) is divisible by the ideal $\mathfrak{D}_{K/K_0} \cdot \text{Norm}_{K/K_0}(\langle \alpha, \beta \rangle)^{2d-2}$ and, in particular:

$$\text{Norm}_{K_0/\mathbb{Q}}(P) \geq \text{Norm}(\mathfrak{D}_{K/K_0}) \text{Norm}_{K/\mathbb{Q}}(\langle \alpha, \beta \rangle)^{2d-2}.$$

³That is: $H(y, (y)) = H(y) := \prod_v \max(|y|_v, 1)$ where the product is taken over all places of K , and $|y|_v$ is normalized to be the multiplicative factor by which $x \mapsto xy$ affects Haar measure on the completion K_v .

⁴Let w be a finite place of K_0 . For arbitrary $e_1, \dots, e_d \in K$, linearly independent over K_0 , with \mathcal{O}_{K_0} -span L , the lattice L^* is the \mathcal{O}_{K_0} -span of the dual basis f_1, \dots, f_d . Write $e_i = \sum_j a_{ij} f_j$. If $L^* \supset L$, then the a_{ij} are all integral, and the w -valuation of $\text{ind}(L^*/L)$ coincides with the w -valuation of the determinant of the matrix (a_{ij}) . But $a_{ij} = \text{Tr}_{K/K_0}(e_i e_j)$. This is the product of the matrix $\{\sigma_i(e_j)\}$ with its transpose, where σ_i ranges over the embeddings of K into a fixed algebraic closure of K_0 . The claimed assertion follows from this and Vandermonde's determinant formula.

However, a direct computation of archimedean sizes in the definition (2.3) shows that

$$|\mathrm{Norm}_{K_0/\mathbb{Q}}(P)| \ll_{[K:\mathbb{Q}]} H_\infty(\alpha : \beta)^{2d-2}$$

where $H_\infty(\alpha : \beta) = \prod_{\sigma \in M_K} \max(|\alpha|_\sigma, |\beta|_\sigma)$. We conclude that

$$H_\infty(\alpha : \beta)^{2d-2} \mathrm{Norm}_{K/\mathbb{Q}}(\langle \alpha, \beta \rangle)^{-2d+2} \gg_{[K:\mathbb{Q}]} \mathrm{Norm}(\mathfrak{D}_{K/K_0})$$

but it is easy to verify that $H(\lambda) = H_\infty(\alpha : \beta) \mathrm{Norm}_{K/\mathbb{Q}}(\langle \alpha, \beta \rangle)^{-1}$. ■

Note that in the analogous case where $K = \mathbb{F}_q(t)$, Lemma 2.2 corresponds to the following fact: if a curve C has a degree d map f to \mathbb{P}^1 , and if $g : C \rightarrow \mathbb{P}^1$ is another map such that the map $f \times g : C \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$ is a birational embedding, then $\deg(g) \geq \frac{g(C)}{d-1} + 1$. (This follows from application of the adjunction formula for curves on $\mathbb{P}^1 \times \mathbb{P}^1$.)

2.3 Use of small noninert primes

If \mathfrak{p} is any fractional ideal of K , we can choose a “preferred representative” $\tilde{\mathfrak{p}} \in \widetilde{\mathrm{Div}}_K^0$ by setting $\tilde{\mathfrak{p}} = (\mathrm{Norm}(\mathfrak{p})^{1/d}, \mathfrak{p})$. Here $\mathrm{Norm}(\mathfrak{p})^{1/d} \in \mathbb{R}$ is considered as an element of K_∞ via the inclusion $\mathbb{R} \hookrightarrow K_\infty$. Then the class of $\tilde{\mathfrak{p}}$ in $\widetilde{\mathrm{Cl}}_K$ projects to the ideal class of \mathfrak{p} under the exact sequence (2.1).

Lemma 2.3. Suppose K/K_0 is an extension of number fields of degree d , let ℓ be a positive integer, and let $\delta < \frac{1}{2\ell(d-1)}$. Suppose that $\{\mathfrak{p}_1, \dots, \mathfrak{p}_M\}$ are prime ideals of norm at most $\mathrm{Norm}(\mathfrak{D}_{K/K_0})^\delta$ that are unramified and are not extensions of prime ideals from any proper subfield of K containing K_0 .

$$\text{Then } \#\mathrm{Cl}_K[\ell] \ll_{[K:\mathbb{Q}], \epsilon, \ell} (\mathrm{disc} K)^{1/2+\epsilon} M^{-1}. \quad \square$$

Proof. Let G be the group $\widetilde{\mathrm{Div}}_K^0$, let P be the group K^\times , and let P_ℓ be $\ell G + P$. Then $\widetilde{\mathrm{Cl}}_K = G/P$ and $\widetilde{\mathrm{Cl}}_K/\ell\widetilde{\mathrm{Cl}}_K = G/P_\ell$. Note that $\widetilde{\mathrm{Cl}}_K[\ell]$ and $\widetilde{\mathrm{Cl}}_K/\ell\widetilde{\mathrm{Cl}}_K$ are finite groups; in view of (2.1), both of them have order that differs from $\#\mathrm{Cl}_K[\ell]$ by $O_{[K:\mathbb{Q}]}(1)$. So to bound $\#\mathrm{Cl}_K[\ell]$ above it suffices to bound $\mathrm{vol}(P_\ell/P)$ from below.

Let T be the subset of G consisting of all elements of the form (x, J) where J is one of the \mathfrak{p}_i and x satisfies

$$2^{-1/\ell} < |x|_{v_1}/|x|_{v_2} < 2^{1/\ell}$$

for all v_1, v_2 in M_K .

Set $T^\ell := \{t^\ell : t \in T\}$. We claim that the map $T^\ell \rightarrow \widetilde{\text{Cl}}_K$ has finite fibers, of size bounded by a constant depending only on $[K : \mathbb{Q}]$. To see this, suppose that $t_1, t_2 \in T$ are such that $u := t_1^\ell t_2^{-\ell}$ lies in K^\times .

Evidently the height of u is $\ll_{[K:\mathbb{Q}]} \text{Norm}(\mathfrak{D}_{K/K_0})^{\ell\delta}$. So $K_1 := K_0(u)$ is a proper subfield of K if $\text{Norm}(\mathfrak{D}_{K/K_0})$ is sufficiently large, by Lemma 2.2. Note that it suffices to prove the Lemma for $\text{Norm}(\mathfrak{D}_{K/K_0})$ larger than any specified function of $[K : \mathbb{Q}], \ell$, so we may assume that indeed it is “sufficiently large” in this sense.

But the nonarchimedean part of u is now a fractional ideal in K_1 which has valuation 0 everywhere, since the \mathfrak{p}_i are not induced from K_1 by hypothesis; so u lies in $\mathcal{O}_{K_1}^\times$. Now any nontrivial $u \in \mathcal{O}_{K_1}^\times$, which is not a root of unity, has an Archimedean valuation of size at least $c = c_{[K:\mathbb{Q}]} > 1$. (Indeed, the set of algebraic integers of degree $\leq A$ and with all archimedean valuations $\leq B$ is finite, which implies the stated assertion.) It follows that the number of $u \in \mathcal{O}_{K_1}^\times$ in the archimedean region defined by the inequalities $1/4 < (|u|_{v_1}/|u|_{v_2}) < 4$ is bounded by a constant depending only on $[K : \mathbb{Q}]$.

But $T^\ell \subset P_\ell$, so what we have shown is that

$$\text{vol}(P_\ell/P) \gg_{[K:\mathbb{Q}]} \text{vol}(T^\ell).$$

Now the volume of T^ℓ is at least $c_{\ell,[K:\mathbb{Q}]} M$ (where the constant $c_{\ell,[K:\mathbb{Q}]}$ keeps track of the volume of the ball cut out by the archimedean conditions.) This proves the proposition. \blacksquare

Remark 2.4. At the suggestion of the referee, let us briefly discuss the idea of Lemma 2.3 in explicit terms, in the case of quadratic fields. The content of the remark that follows is entirely due to the referee; we thank him for allowing us to include it.

We explain the idea in nonquantitative terms.

Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field, σ the nontrivial automorphism of K , $\varepsilon > 1$ the fundamental unit. We shall choose an embedding of K into \mathbb{R} and regard K as a subfield of \mathbb{R} thereby.

We define a homomorphism Θ from the group of fractional ideals whose ℓ th power is principal, to $\mathbb{R}/\log(\varepsilon)\mathbb{Z}$, in the following fashion: to each fractional ideal \mathfrak{J} whose ℓ th power is principal and generated by $\alpha \in K^\times$, we assign $\Theta(\mathfrak{J}) := \log(|\frac{\alpha}{\sigma(\alpha)}|)$.

Suppose p, q are “small” distinct primes in \mathbb{Z} which split in K : so $(p) = \mathfrak{p}\mathfrak{p}^*$, $(q) = \mathfrak{q}\mathfrak{q}^*$. If $\mathfrak{p}, \mathfrak{q}$ belong to the same coset of $\text{Cl}_K[\ell]$, then

$$\Theta(\mathfrak{p}\mathfrak{q}^{-1}) \text{ cannot be close to zero inside } \mathbb{R}/\log(\varepsilon)\mathbb{Z}. \tag{2.4}$$

For, noting that $\Theta(\mathfrak{p}q^{-1}) = \Theta(\mathfrak{p}q^*)$, it would otherwise mean that $\mathfrak{p}^\ell(q^*)^\ell$ is generated by an element α so that $\sigma(\alpha)$ is very close to $\pm\alpha$. This cannot happen when p, q are very small compared to \sqrt{d} .

Now suppose we are given a large subset p_1, \dots, p_M of small primes in \mathbb{Z} , all of which split in K ; let \mathfrak{p}_j be a prime ideal above p_j . Then there exists a subset of $\{\mathfrak{p}_1, \dots, \mathfrak{p}_M\}$ with size $\geq \lfloor \frac{M}{\#\text{Cl}_K[\ell]} \rfloor$, all of whom belong to the same coset of $\text{Cl}_K[\ell]$. By the pigeonhole principle, applied to $\Theta(\mathfrak{p}_i\mathfrak{p}_1^{-1})$, there will exist $\mathfrak{p}_i, \mathfrak{p}_j$ so that $\Theta(\mathfrak{p}_i\mathfrak{p}_j^{-1})$ is very close to zero. If $\frac{M}{\#\text{Cl}_K[\ell]}$ is too big, this will contradict (2.4).

Quantifying this yields an explicit proof of the Lemma.

3 Bounds on ℓ -torsion, conditional and unconditional

3.1 Conditional bounds under GRH

Proposition 3.1. Let K be an extension of \mathbb{Q} of degree d . Then, assuming GRH,

$$\#\text{Cl}_K[\ell] \ll_{d,\epsilon} (\text{disc } K)^{1/2 - \frac{1}{2\ell(d-1)} + \epsilon}. \quad \square$$

Proof. The proof is immediate from Lemma 2.3, together with the “effective Chebotarev” theorem of Lagarias and Odlyzko [11] which, subject to GRH, guarantees for any $\eta > 0$ the existence of $\gg (\text{disc } K)^{\eta - \epsilon}$ primes of \mathbb{Q} of size $\leq (\text{disc } K)^\eta$ which split completely in K . ■

3.2 A version of the reflection principle

We turn now to unconditional bounds. As remarked, producing “small” split primes in a number field without GRH is a major problem in analytic number theory; in particular there is little hope of an unconditional result via direct application of Prop. 3.1. The main idea is to use a weak (but fairly general) form of the Scholz reflection principle.

The idea can be most clearly seen in the analogous case where K is the function field of a curve C/\mathbb{F}_q ; the ℓ -torsion in the Arakelov class group of K is then just $\text{Jac}(C)[\ell](\mathbb{F}_q)$. Now $\text{Jac}(C)[\ell](\bar{\mathbb{F}}_q)$ admits a μ_ℓ -valued symplectic pairing (the Weil pairing); this splits the Frobenius eigenspaces on $\text{Jac}(C)[\ell](\bar{\mathbb{F}}_q)$ into pairs of dual eigenspaces. If the Frobenius acts nontrivially on μ_ℓ , then this shows that the Frobenius-fixed eigenspace $\text{Jac}(C)[\ell](\mathbb{F}_q)$ has the same dimension as the eigenspace where Frobenius acts as multiplication by q . In particular, when $q \cong -1(\ell)$ one has that Frobenius has equally many $+1$ and -1 eigenvalues on $\text{Jac}(C)[\ell](\bar{\mathbb{F}}_q)$.

The number field version of this argument yields reflection principles: a good account of much more general and precise theorems of this form than those used here can be found in the article of Gras [12].

Lemma 3.2. Let $\ell > 2$ be a prime and ζ_ℓ an ℓ th root of unity. Let $K_0 = \mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$, and let K be an extension of K_0 which does not contain ζ_ℓ . Let $L = K(\zeta_\ell)$, which is a quadratic extension of K . Let Cl^+ and Cl^- be, respectively, the positive and negative eigenspaces for the action of $\text{Gal}(L/K)$ on $\text{Cl}_L[\ell]$. Then

$$|\text{rank Cl}^+ - \text{rank Cl}^-| \leq O_{[L:\mathbb{Q}]}(1). \quad \square$$

In the statement of the Lemma, and in the proof below, rank denotes dimension as a \mathbb{Z}/ℓ -vector space.

Proof. This is standard, but we include a proof here to make the present article self-contained.

Let \tilde{A} be the subgroup of L^\times consisting of elements whose valuations at all primes are multiples of ℓ , and let $A = \tilde{A}/(L^\times)^\ell$. Then there is a surjection

$$A \rightarrow \text{Cl}_L[\ell]$$

which sends x to the class of the fractional ideal whose ℓ 'th power is (x) . The kernel of this map is $\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^\ell$, whose dimension is $O_{[L:\mathbb{Q}]}(1)$.

Let L' be the field obtained by adjoining $x^{1/\ell}$ to L for all $x \in \tilde{A}$, and let $B = \text{Gal}(L'/L)$. Then A is naturally identified (as $\text{Gal}(L/K)$ -module) with $\text{Hom}(B, \mu_\ell)$ by Kummer theory, i.e.:

$$x \in A \mapsto (\sigma \in B \mapsto (x^{1/\ell})^\sigma (x^{1/\ell})^{-1}) \in \text{Hom}(B, \mu_\ell).$$

On the other hand, let G be the Galois group of the maximal abelian ℓ -extension of L unramified away from ℓ . Since L' is contained in this abelian ℓ -extension, G naturally surjects onto B , and the kernel of this map has \mathbb{F}_ℓ -dimension $O_{[L:\mathbb{Q}]}(1)$ by a consideration of inertia at ℓ .

What's more, by class field theory, G differs from $\text{Cl}_L \otimes_{\mathbb{Z}} \mathbb{Z}/\ell$ (in the Grothendieck group of the category of $\mathbb{F}_\ell[\text{Gal}(L/K)]$ -modules) by a representation of dimension $O_{[L:\mathbb{Q}]}(1)$. Thus, up to representations of dimension $O_{[L:\mathbb{Q}]}(1)$, we have

$$\text{Cl}_L[\ell] \cong \text{Hom}(\text{Cl}_L \otimes_{\mathbb{Z}} \mathbb{Z}/\ell, \mu_\ell) = \text{Hom}(\text{Cl}_L, \mu_\ell).$$

Now, $\text{Gal}(L/K)$ acts by -1 on μ_ℓ and so this means precisely that the positive and negative eigenspaces of $\text{Gal}(L/K)$ on $\text{Cl}_L[\ell]$ differ in dimension by $O_{[L:\mathbb{Q}]}(1)$, as claimed.

It is worth making explicit how this implies (a slightly weaker version of) the usual Scholz reflection principle:

Lemma 3.3. Let E be a fixed number field, $K = E(\sqrt{\eta})$ a quadratic extension of E not containing $\sqrt{-3}$. Then

$$|\text{rank Cl}_{E(\sqrt{-3\eta})}[3] - \text{rank Cl}_{E(\sqrt{\eta})}[3]| \leq O_{[E:\mathbb{Q}]}(1) \quad (3.1)$$

□

Proof. Set $L = E(\sqrt{\eta}, \sqrt{-3}) = K(\zeta_3)$.

Let χ_1 be the nontrivial character of $\text{Gal}(K/E)$, and let χ_2 be the nontrivial character of $\text{Gal}(E(\sqrt{-3})/E)$. We regard them both as characters of $\text{Gal}(L/E)$. Then $\text{Cl}_L[3]$ splits as a direct sum of eigenspaces:

$$\text{Cl}_L[3] = \text{Cl}_L[3]^1 \oplus \text{Cl}_L[3]^{\chi_1} \oplus \text{Cl}_L[3]^{\chi_2} \oplus \text{Cl}_L[3]^{\chi_1\chi_2}$$

where, for any character ψ of $\text{Gal}(L/E)$, the notation $\text{Cl}_L[3]^\psi$ denotes $\{x \in \text{Cl}_L[3] : gx = \psi(g)x, \forall g \in \text{Gal}(L/E)\}$. In this language, Lemma 3.2 says precisely that the rank of $\text{Cl}_L[3]^1 \oplus \text{Cl}_L[3]^{\chi_1}$ and the rank of $\text{Cl}_L[3]^{\chi_2} \oplus \text{Cl}_L[3]^{\chi_1\chi_2}$ differ by $O_{[E:\mathbb{Q}]}(1)$. The same is true for $\text{Cl}_L[3]^1 \oplus \text{Cl}_L[3]^{\chi_1\chi_2}$ and $\text{Cl}_L[3]^{\chi_1} \oplus \text{Cl}_L[3]^{\chi_2}$; it follows that the ranks of $\text{Cl}_L[3]^{\chi_1}$ and $\text{Cl}_L[3]^{\chi_1\chi_2}$ differ by $O_{[E:\mathbb{Q}]}(1)$, which implies the stated result.

3.3 Unconditional bounds for ℓ -torsion

We begin with the most concrete application, which is to quadratic fields.

Proposition 3.4. Let D be a squarefree integer. The 3-torsion part of the class group of $\mathbb{Q}(\sqrt{D})$ has size $\ll_\epsilon |D|^{1/3+\epsilon}$. □

Proof. Any prime not dividing $6D$ which is inert in $\mathbb{Q}(\sqrt{-3})$ splits in either $\mathbb{Q}(\sqrt{D})$ or $\mathbb{Q}(\sqrt{-3D})$. In particular, for at least one $d \in \{D, -3D\}$ there are $\gg |d|^{1/6-2\epsilon}$ primes $p \in [d|^{1/6-\epsilon}, 2d|^{1/6-\epsilon}]$ which split in $\mathbb{Q}(\sqrt{d})$. This shows, via Lemma 2.3, that the size of the 3-torsion part of the class group of $\mathbb{Q}(\sqrt{d})$ is $\ll |d|^{1/3+\epsilon}$.

However, Scholz's reflection principle (Lemma 3.3) shows that the 3-ranks of the class groups of $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{-3D})$ differ by a bounded amount (indeed, Scholz's more precise formulation asserts that these differ by at most 1).

The argument above applies much more generally. For instance, if K_0 is a number field which contains $\zeta_\ell + \zeta_\ell^{-1}$ but does not contain ζ_ℓ , then we can bound the ℓ -torsion in the class groups of quadratic extensions $K = K_0(\sqrt{\alpha})$ of K_0 . Note that $K_0(\zeta_\ell)$ is a quadratic extension which may write as $K_0(\sqrt{\beta})$ for some $\beta \in K_0$. Let $\delta < \frac{1}{2\ell}$ and let $X = \text{Norm}(\mathfrak{D}_{K/K_0})^\delta$; then, once X is sufficiently large (depending on K_0) there are on order of $X/\log X$ primes of K_0 with norm below X which are inert in $K_0(\zeta_\ell)/K_0$. Then, as above, Lemma 2.3 applies to either K or $K_0(\sqrt{\alpha\beta})$ (as long as we exclude the case $\alpha = \beta$, which is harmless) and applying Lemma 3.3, one obtains the following:

Proposition 3.5. Let K_0 be a number field which contains $\zeta_\ell + \zeta_\ell^{-1}$ but does not contain ζ_ℓ . Let K/K_0 be a quadratic extension. Then

$$\#\text{Cl}_K[\ell] \ll_{\epsilon, K_0} (\text{disc } K)^{\frac{1}{2} - \frac{1}{2\ell} + \epsilon}. \quad \square$$

We generalize this method to higher degree extensions in the following Proposition.

Proposition 3.6. Let ℓ be an odd prime, $K_0 = \mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$, and let K be an extension of K_0 of even degree $d > 2$ such that $\zeta_\ell \notin K$ and such that the extension $K(\zeta_\ell)/K_0$ has no proper subextensions apart from K and $\mathbb{Q}(\zeta_\ell)$. Then

$$\#\text{Cl}_K[\ell] \ll_{\epsilon, d, \ell} (\text{disc } K)^{1/2 - \frac{1}{2\ell d(2d-1)} + \epsilon}. \quad \square$$

Note that the condition on intermediate subextensions of $K(\zeta_\ell)/K_0$ excludes the case $d = 2$, but we have treated this case immediately above (obtaining a bound better than that of Proposition 3.6).

Proof. Let $L = K(\zeta_\ell)$.

Then:

- (1) $\text{disc}(L) \asymp_\ell \text{disc}(K)^2$; and
- (2) No prime of K_0 , unramified in L , remains inert in L .

Let us verify the second assertion. Let k be a number field with two extensions, k_1, k_2 of degrees d_1, d_2 and linearly disjoint over k , so that the natural map $k_1 \otimes_k k_2 \rightarrow k_3 := k_1.k_2$ is an isomorphism. Fix a finite place w of k and a corresponding embedding $k \hookrightarrow k_w$. Fix an algebraic closure $\overline{k_w}$ of k_w ; let P_i be the set of embeddings of k_i into $\overline{k_w}$ extending the embedding of k . The restriction maps $P_3 \rightarrow P_1$ and $P_3 \rightarrow P_2$ induce a bijection $P_3 \rightarrow P_1 \times P_2$ (bijectivity uses the linear disjointness). The places of k_i above w are

parameterized by $\text{Gal}(\overline{k_w}/k_w)$ -orbits on P_i . Let F be a Frobenius element in this Galois group. The identification of P_3 with $P_1 \times P_2$ respects the Galois-action; so, if F acts with a single orbit on P_3 , then it would also do so on P_1 and P_2 . But then $F^{\text{lcm}(d_1, d_2)}$ acts trivially on P_1, P_2 , so also on P_3 ; a contradiction if d_1, d_2 have a common divisor. Therefore, if $\gcd(d_1, d_2) > 1$ and all places of k_3 above w are unramified, there must exist at least two such places. We apply the observation to $k = K_0, k_1 = K_0(\zeta_\ell), k_2 = K, k_3 = L$.

Let S be the set of primes \mathfrak{p} of K_0 that are unramified in L and inert in $\mathbb{Q}(\zeta_\ell)$. Take $\delta < \frac{1}{\ell d(2d-1)}$ and $X = (\text{Norm}(\mathfrak{D}_{K/K_0}))^\delta$.

Then there are $\gg_{d, \ell} X/\log(X)$ primes \mathfrak{p} in S with norm between $X/2$ and X . Call this set of primes S_X . One of the following possibilities occurs:

- (1) The number of primes in S_X which are inert in K is $\gg_{\ell, d} X/\log X$; or
- (2) The number of primes in S_X which are *not* inert in K is $\gg_{\ell, d} X/\log X$.

Suppose the latter. For each such \mathfrak{p} , there is more than one prime \mathfrak{p}_K of K dividing \mathfrak{p} ; thus there exists such a \mathfrak{p}_K whose norm is at most $X^{d/2} < (\text{Norm}(\mathfrak{D}_{K/K_0}))^{\frac{1}{2\ell(2d-1)}}$. Note that \mathfrak{p}_K cannot come from a proper subextension of K/K_0 , since the only such subextension is K_0 itself by hypothesis, and we have assumed \mathfrak{p} is not inert in K . It follows from Lemma 2.3 that

$$\#\text{Cl}_K[\ell] \ll_{d, \ell, \epsilon} (\text{disc } K)^{1/2-\delta+\epsilon}. \quad (3.2)$$

Now suppose the former, and let \mathfrak{p} be a prime of S which is inert in K ; we have seen it is not inert in L . Let \mathfrak{p}_L be a prime ideal of L dividing \mathfrak{p} . Then \mathfrak{p}_L is not the extension of a prime ideal of $\mathbb{Q}(\zeta_\ell)$, nor the extension of a prime ideal of K : for \mathfrak{p} remains inert in both of these fields. As above, we may thus choose \mathfrak{p}_L to have norm at most

$$X^d < (\text{Norm}(\mathfrak{D}_{K/K_0}))^{\frac{1}{\ell(2d-1)}} \asymp_{\ell, d} (\text{Norm}(\mathfrak{D}_{L/K_0}))^{\frac{1}{2\ell(2d-1)}}.$$

Now another application of Lemma 2.3 yields

$$\#\text{Cl}_L[\ell] \ll_{d, \ell, \epsilon} (\text{disc } L)^{1/2-\delta/2+\epsilon}. \quad (3.3)$$

The (two-element) Galois group $\text{Gal}(L/K)$ acts on $\text{Cl}_L[\ell]$, splitting it into positive and negative eigenspaces, and the positive eigenspace is exactly $\text{Cl}_K[\ell]$. In this context Lemma 3.2 asserts that the ℓ -ranks of these eigenspaces differ by at most $O_{d, \ell}(1)$; so in particular we have

$$\#\text{Cl}_K[\ell] \ll_{d, \ell} \#\text{Cl}_L[\ell]^{1/2}.$$

This, together with the fact that either (3.2) or (3.3) holds, and that $\delta < \frac{1}{\ell d(2d-1)}$ is arbitrary, yields the desired conclusion on $\#\text{Cl}_K[\ell]$.

It is possible that the condition on intermediate subfields might be significantly weakened by techniques similar to those used for the proof of the Corollary that follows. On the other hand, one cannot remove this completely: it is clear that the method of this article fails entirely if $\zeta_\ell \in K$.

We conclude with the following Corollary:

Corollary 3.7. Let K be an extension of \mathbb{Q} with $[K : \mathbb{Q}] = d \leq 4$. Then there is $\delta = \delta(d) > 0$ so that the 3-torsion part of the class group $\text{Cl}_K[3]$ satisfies the bound

$$\#\text{Cl}_K[3] \ll \text{disc}(K)^{1/2-\delta(d)}.$$

Any $\delta(2) = \delta(3) < 1/6$ is admissible. □

Proof. Most cases follow quite easily from our results and existing results about cubic fields. Indeed, most of the proof will be concerned with dealing with the “nongeneric” case of quadratic extensions of a quadratic field.

- (1) If K is quadratic, we may apply Proposition 3.4 directly.
- (2) If K is a noncyclic cubic extension, we apply the main result of [13] to reduce the question to that of the 3-torsion of the quadratic resolvent.⁵
- (3) If K is a cyclic cubic extension, then one has much better bounds through a suitable generalization of Gauss’ genus theory. Indeed, if t is the number of ramified primes of K , the 3-rank is $\ll t$. This implies $\#\text{Cl}_K[3] \ll_\epsilon (\text{disc } K)^\epsilon$.
- (4) If K is a quartic extension of \mathbb{Q} such that $\zeta_3 \notin K$ and $K(\zeta_3)$ has no subfields other than $K, \mathbb{Q}(\zeta_3)$, and \mathbb{Q} , Proposition 3.6 shows that $\#\text{Cl}_K[3] \ll \text{disc}(K)^{1/2-\delta}$ for some $\delta > 0$.

If the Galois group attached to K/\mathbb{Q} is A_4 or S_4 , then $K(\zeta_3)$ has no unexpected subfields and we are in the case treated above. It remains to deal with the case when K is quartic and contains a quadratic subfield $E = \mathbb{Q}(\sqrt{d})$. In that case, $K = E(\sqrt{\eta})$ for some $\eta \in E$. The basic idea is this: we show that $\text{Cl}_K[3]$ is small *either* by showing $\text{Cl}_E[3]$ is small – this is enough if $|d|$ is large compared to $\text{disc } K$ – *or* by treating K as a quadratic extension of E , thinking of E as “almost fixed”, and applying Lemma 2.3 to the extension K/E .

⁵We thank J. Klüners for bringing this type of result to our attention.

Let σ be the nontrivial element of $\text{Gal}(K/E)$ and let $\text{Cl}_K^\pm = \{x \in \text{Cl}_K : x^\sigma = x^{\pm 1}\}$. The natural map $\text{Cl}_K^+ \times \text{Cl}_K^- \rightarrow \text{Cl}_K$ induces an isomorphism $\text{Cl}_K[3] = \text{Cl}_K^+[3] \times \text{Cl}_K^-[3]$. There is a natural map, induced by extension of ideals,

$$\iota : \text{Cl}_E \rightarrow \text{Cl}_K^+, \quad (3.4)$$

which induces an isomorphism⁶ on 3-torsion; in particular, $\#\text{Cl}_K^+[3] \ll_\epsilon |d|^{1/3+\epsilon}$.

To bound the size of Cl_K^- , we use the natural map $\text{Cl}_E \xrightarrow{\iota} \text{Cl}_K \rightarrow \text{Cl}_K/\text{Cl}_K^-$; the cardinality of the kernel is at most the size of the 2-torsion of Cl_E , which has size $|d|^\epsilon$ by genus theory. Thus $\#\text{Cl}_E \cdot \#\text{Cl}_K^- \ll_\epsilon |d|^\epsilon \cdot \#\text{Cl}_K$. On the other hand, if R_K and R_E denote the regulator of K and E respectively, we have the Brauer–Siegel bound $\frac{R_K \cdot \#\text{Cl}_K}{R_E \cdot \#\text{Cl}_E} \ll_\epsilon (\text{disc } K)^{1/2+\epsilon} |d|^{-1/2}$.

One verifies that $R_K \gg R_E$: indeed, let M_K, M_E be the set of infinite places of K, E respectively. σ acts on M_K and the orbits are identified with M_E ; therefore, we can identify \mathbb{R}^{M_E} with the σ -fixed space in \mathbb{R}^{M_K} . Then the unit groups of K, E embed as lattices U_K, U_E within the subspaces $\{x_v : \sum x_v = 0\}$ inside $\mathbb{R}^{M_K}, \mathbb{R}^{M_E}$ respectively. Let U_K^- be the $-$ eigenspace of σ on U_K . The decomposition $2x = (x + \sigma(x)) + (x - \sigma(x))$ shows that the index of $U_E \oplus U_K^-$ inside U_K is $\leq 2^{\text{rank}_{\mathbb{Z}} U_K} \leq 8$. Since U_E, U_K^- are orthogonal inside \mathbb{R}^{M_K} we conclude that

$$R_K/R_E \asymp \text{vol}(U_K^- \otimes \mathbb{R}/U_K^-),$$

the volume being taken w.r.t. the Euclidean metric on \mathbb{R}^{M_K} . As in the proof of Lemma 2.3, the archimedean valuation of any element in U_K^- that is not a root of unity is bounded away from 1. In particular, there is an absolute constant c so that any element of U_K^- has length $\geq c$ w.r.t. the Euclidean metric. This means that $\text{vol}(U_K^- \otimes \mathbb{R}/U_K^-) \gg 1$.

Therefore $\#\text{Cl}_K^- \ll (\text{disc } K)^{1/2+\epsilon} |d|^{-1/2+\epsilon}$.

We conclude that

$$\#\text{Cl}_K[3] \ll_\epsilon (\text{disc } K)^{1/2+\epsilon} |d|^{-1/6} \quad (\mathbb{Q}(\sqrt{d}) \subset K). \quad (3.5)$$

(3.5) is sufficient to give a nontrivial bound if d is large compared to $\text{disc}(K)$, but we still need to obtain a good bound when d is small relative to $\text{disc}(K)$. The idea is to treat K as a quadratic extension of $E = \mathbb{Q}(\sqrt{d})$ and, if $\sqrt{-3} \notin K$, proceed as in Proposition 3.5, but this time paying attention to the dependence on E . It is clear, in view of (3.5), that we will

⁶To see this, note that, on prime-to-2 components, the inclusion (3.4) is split by the norm map $\text{Cl}_K \rightarrow \text{Cl}_E$.

have the desired result so long as we can show

$$\#\mathrm{Cl}_K[3] \ll_{\epsilon} \mathrm{disc}(K)^{1/2-\delta} |d|^A \quad (3.6)$$

for some positive δ, A .

(1) The case $\sqrt{-3} \notin K$.

In order to do this, we note that, if $p \in [X/2, X]$ is any (rational) prime which is split in $\mathbb{Q}(\sqrt{d})$ but inert in $\mathbb{Q}(\sqrt{-3})$, then any prime \mathfrak{p}_E above p remains inert in $E(\sqrt{-3})$. In particular, such a prime \mathfrak{p}_E splits in either $E(\sqrt{\eta})$ or $E(\sqrt{-3\eta})$. Using a quantitative version of Linnik's theorem on primes in arithmetic progression [14, Cor. 18.8], we see that there are at $\gg_{\epsilon} X^{1-\epsilon} |d|^{-3/2}$ such primes \mathfrak{p}_E , as long as $X \geq |d|^L$. Here L is an absolute constant.

Assume henceforth that $X \geq |d|^L$. We have shown that for at least one $\eta' \in \{\eta, -3\eta\}$, there exists $\gg_{\epsilon} X^{1-\epsilon} |d|^{-3/2}$ primes $\mathfrak{p}_{E(\sqrt{\eta'})}$ in $E(\sqrt{\eta'})$, of norm in $[X/2, X]$, which are not extensions of prime ideals from E . By Lemma 3.3, we know that $\#\mathrm{Cl}_K[3] \ll \#\mathrm{Cl}_{E(\sqrt{\eta'})}[3]$. We can apply Lemma 2.3 to the extension $E(\sqrt{\eta'})/E$ as long as $X < \mathrm{Norm}(\mathfrak{D}_{E(\sqrt{\eta'})/E})^{1/6.01}$, which is possible once $\mathrm{disc} K$ is greater than some large power of $|d|$. Carrying this out yields (3.6).

(2) The case of $\sqrt{-3} \in K$. To deal with that case, the methods of this article do not suffice, but the result of [4] is also valid over a number field (this is remarked in the introduction to [4], although a full proof over a number field is not written). Thus, if K contains $\sqrt{-3}$, we treat K as a quadratic extension of $\mathbb{Q}(\sqrt{-3})$ and obtain the bound

$$\#\mathrm{Cl}_K[3] \ll (\mathrm{disc} K)^{0.45} \quad (\sqrt{-3} \in K). \quad (3.7)$$

Acknowledgments

We are very grateful to both Soundararajan and Michel for their generosity in discussing the idea of using small split primes to bound class groups. We would also like to thank the referee for a particularly careful reading of the article and a large number of very useful comments.

The first author was partially supported by NSF-CAREER Grant DMS-0448750 and a Sloan Research Fellowship; the second author was supported by a Clay research fellowship, NSF Grant DMS-0245606 and NSF Grant DMS-0111298; he also thanks the Institute for Advanced Study for providing superb working conditions. We thank the Clay Mathematics Institute for supporting a visit of

the second author to the University of Wisconsin in November 2005, during which most of the ideas in this article were developed.

References

- [1] Duke, W. "Bounds for arithmetic multiplicities." *Proceedings of the International Congress of Mathematicians*. Berlin, 1998.
- [2] Zhang, S.-W. "Equidistribution of CM-points on quaternion Shimura varieties." *International Mathematics Research Notices* 59 (2005): 3657–3689.
- [3] Brumer, A., and J. Silverman. "The number of elliptic curves over \mathbb{Q} with conductor N ." *Manuscripta Mathematica* 91, no. 1 (1996): 95–102.
- [4] Helfgott, H., and A. Venkatesh. "Integral points on elliptic curves and 3-torsion in class groups." *Journal of the American Mathematical Society* 19, no. 3 (2006): 527–550.
- [5] Pierce, L. "The 3-part of class numbers of quadratic fields." *Journal of the London Mathematical Society (2)* 71 (2005): 579–598.
- [6] Ellenberg, J., and A. Venkatesh. "Counting extensions of function fields with bounded discriminant and specified Galois group." *Geometric Methods in Algebra and Number Theory*, Progress in Math 235, Boston, MA: Birkhuser Boston, (2005): 151–168.
- [7] Boyd, D., and H. Kisilevsky. "On the exponent of the ideal class groups of complex quadratic fields." *Proceedings of the American Mathematical Society* 31 (1972): 433–436.
- [8] Madan, M., and D. Madden. "Note on the class group of algebraic function fields." *Journal Fur Die Reine Und Angewandte Mathematik* 295 (1977): 57–60.
- [9] Soundararajan, K. "Divisibility of class numbers of imaginary quadratic fields." *Journal of the London Mathematical Society-Second Series* 61, no. 3 (2000): 681–690.
- [10] Schoof, R. "Arakelov Class Groups, by J. Voight." Lecture notes. <http://websites.math.leidenuniv.nl/algebra>.
- [11] Lagarias, J., and A. Odlyzko. "Effective versions of the Chebotarev density theorem." *Algebraic Number Fields: L-functions and Galois Properties*, 409–464. Durham: Processing Symposium University Durham, 1975.
- [12] Gras, G. "Théoremes de réflexion." *Journal Théorie des Nombres de Bordeaux* 10, no. 2 (1998): 399–499.
- [13] Gerth, F. III. "Ranks of 3-class groups of non-Galois cubic fields." *Acta Arithmetica* 30, no. 4 (1976): 307–322.
- [14] Iwaniec, H., and E. Kowalski. *Analytic Number Theory*, Colloquium Publications, Vol. 53: American Mathematical Society, Providence, Rhode Island, 2004.