LOWER BOUNDS FOR THE LEAST PRIME IN CHEBOTAREV

ANDREW FIORI

Abstract. In this paper we show there exists an infinite family of number fields $L$, Galois over $\mathbb{Q}$, for which the smallest prime $p$ of $\mathbb{Q}$ which splits completely in $L$ has size at least $(\log(|D_L|))^{2+o(1)}$. This gives a converse to various upper bounds, which shows that they are best possible.

1. Introduction

The purpose of this note is to prove the following result.

Theorem 1. There exists an infinite family of number fields $L$, Galois over $\mathbb{Q}$, for which the smallest prime $p$ of $\mathbb{Q}$ which splits completely in $L$ has size at least

$$(1 + o(1)) \left( \frac{3e^\gamma}{2\pi} \right)^2 \left( \frac{\log(|D_L|) \log(2 \log \log(|D_L|))}{\log \log(|D_L|)} \right)^2$$

as the absolute discriminant $D_L$ of $L$ over $\mathbb{Q}$, tends to infinity.

The result is independent of the Generalized Riemann Hypothesis. The result complements the existing literature on what is essentially a converse problem, stated generally as

Problem. Let $K$ be a number field, and $L$ be a Galois extension of $K$, for any conjugacy class $C$ in $\Gamma(L/K)$, the Galois group of $L/K$, show that the smallest (in norm) unramified degree one prime $p$ of $K$ for which the conjugacy class $\text{Frob}_p$ is $C$ is small relative to $|D_L|$, the absolute discriminant of $L/K$.

Solutions to this problem have important applications in the explicit computation of class groups (see [3]) where smaller is better. Some of the history of just how small we can get is summarized below:

- Lagarias and Odlyzko showed $N_{K/\mathbb{Q}}(p) < (\log(|D_L|))^{2+o(1)}$ conditionally on GRH (see [8]).
- Bach and Sorenson gave an explicit constant $C$ so that $N_{K/\mathbb{Q}}(p) < C (\log(|D_L|))^2$ conditionally on GRH (see [2]).
- Lagarias, Montgomery, and Odlyzko showed there is a constant $A$ such that $N_{K/\mathbb{Q}}(p) < |D_L|^A$ (see [7]).
- Zaman showed $N_{K/\mathbb{Q}}(p) < |D_L|^{10}$ for $D_L$ sufficiently large (see [12]).
- Kadiri, Ng and Wong improved this to $N_{K/\mathbb{Q}}(p) < |D_L|^{16}$ for $D_L$ sufficiently large (see [6]).
- Ahn and Kwon showed $N_{K/\mathbb{Q}}(p) < |D_L|^{12577}$ for all $L$ (see [1]).

By the above, Theorem 1 and the GRH bound above are best possible up to the exact $o(1)$ term.

Remark. The family under consideration will be a subfamily of the Hilbert class fields of quadratic imaginary extensions of $\mathbb{Q}$. All of the Galois groups will be generalized dihedral groups, and in the family the degree of the extensions goes to infinity.

We also would like to point out the work of Sandari (see [11, Sec. 1.3]) where some similar features of this family are remarked on in a different context.

2010 Mathematics Subject Classification. Primary 11R44; Secondary 11R29.

The author thanks the University of Lethbridge for providing a stimulating environment to conduct this work and in particular Nathan Ng and Habiba Kadiri for directing him towards this project. The author would also like to thank the referee whose suggestions simplified the proof of our main result.
2. Proofs

We first recall a few basic facts from algebraic number theory and class field theory.

**Lemma 2.** Let $K = \mathbb{Q}(\sqrt{-d})$ where $d = |\text{disc}(K)|$, let $\mathfrak{p}$ be a principal prime ideal of $K$. If we have $N_{K/\mathbb{Q}}(\mathfrak{p}) = (p)$ then $p$ is a norm of $\mathcal{O}_K$ and hence $p \geq d/4$.

**Proof.** Assuming $\mathfrak{p}$ is principally generated by $x$, then $N_{K/\mathbb{Q}}(\mathfrak{p})$ is principally generated by $N_{K/\mathbb{Q}}(x)$. As norms from $K$ are positive, this gives that $p$ must be a norm.

We next note that for $x + y\sqrt{-d} \in \mathcal{O}_K$ the expression $N_{K/\mathbb{Q}}(x + y\sqrt{-d}) = x^2 + dy^2$ cannot be prime if $y = 0$. Now, because $\mathcal{O}_K \subset \frac{1}{4}\mathbb{Z} + \frac{\sqrt{-d}}{4}\mathbb{Z}$ we conclude that if the norm is a prime, then $y \geq \frac{1}{2}$, from which it follows that if $p$ is a norm then $p \geq d/4$. \qed

**Lemma 3.** Let $K = \mathbb{Q}(\sqrt{-d})$ where $d = |\text{disc}(K)|$, suppose that $H$ is the Hilbert class field of $K$. If $p$ is a prime of $\mathbb{Z}$ which splits completely in $H$, then $p$ splits in $K$ as $(p) = \mathfrak{p}_1\mathfrak{p}_2$ where both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are principal and $N_{K/\mathbb{Q}}(\mathfrak{p}_i) = (p)$. In particular, by the previous lemma $p \geq d/4$.

**Proof.** The first claim is clear because ramification degrees, inertia degrees and hence splitting degrees are multiplicative in towers. That $\mathfrak{p}_i$ must be principal is a consequence of class field theory. Principal ideals for $\mathcal{O}_K$ map to the trivial Galois element for the Galois group of the Hilbert class field. However, for unramified prime ideals this map gives Frobenius. As the Frobenius element is trivial precisely when the inertial degree is 1, equivalently for Galois fields when the prime splits completely, we conclude the result. \qed

**Remark 4.** Denote by $\chi_d$ the quadratic Dirichlet character with fundamental discriminant $-d$. The main idea of the proof is to use the class number formula with lower bounds for $L(1, \chi_d)$. Using Siegel’s ineffective bound gives

$$d = h_K^{2+o(1)} = \log |D_H|^{2+o(1)}.$$  

To obtain our precise result we refine the $o(1)$ term using extreme values of $L(1, \chi_d)$.

**Lemma 5.** Let $K = \mathbb{Q}(\sqrt{-d})$ where $d = |\text{disc}(K)| > 16$, suppose that $H$ is the Hilbert class field of $K$. Then

$$\log |D_H| = h_K \log(d) = \frac{1}{\pi} L(1, \chi_d) \sqrt{d} \log(d)$$

where $h_K$ is the class number of $K$, $D_H$ is the discriminant of $H$ and $\chi_d$ is the quadratic Dirichlet character with fundamental discriminant $-d$.

**Proof.** The first equality is immediate from the multiplicativity of the discriminant in towers, the second follows from the analytic class number formula

$$h_K = \frac{\sqrt{d}}{\pi} L(1, \chi_d).$$  

The estimates on the extreme values of $L(1, \chi_d)$ which we need are the following.

**Theorem 6.** There exists a family of quadratic imaginary fields $K = \mathbb{Q}(\sqrt{-d})$ where $d = |\text{disc}(K)|$ such that for $\chi_d$, the quadratic Dirichlet character with fundamental discriminant $-d$, we have

$$L(1, \chi_d) < (1 + o(1)) \frac{\pi^2}{6e\gamma \log \log(d)}.$$  

A result of this sort was originally proven by Littlewood conditional on the generalized Riemann hypothesis (see [9]), his result was proven unconditionally by Paley (see [10]) the version stated here follows from the work of Chowla (see [4]). It is possible that the work of Granville and Soundararajan (see [5]) can further refine the constants in the above, and consequently those in Theorem [11].

The following proof includes several significant simplifications suggested by the referee. We would like to thank them for these valuable suggestions.
Proof of Theorem 1. We consider the family of fields $L = H_K$ where $K$ is a field from the infinite family of Theorem 6 for which $d > 16$. To complete the proof we introduce some notation, define  

$$x_d = L(1, \chi_d) \log \log(d) \quad \text{and} \quad f_d(x) = \frac{x\sqrt{d} \log(d)}{\pi \log \log(d)}.$$ 

Then by our choice of $d$ we have  

$$x_d < \frac{\pi^2}{6e^7} + o(1)$$

and by Lemma 5 we have  

$$\log |D_L| = f_d(x_d).$$

Now because the function $y \mapsto \frac{y \log(2 \log(y))}{\log(y)}$ is increasing for $y > e$ and as  

$$f_d(x_d) = \log |D_L| = h_K \log(d) \geq \log(16) > e$$

it follows that  

$$\frac{\log |D_L|}{\log \log |D_L|} \leq \frac{f_d(x_d) \log(2 \log(f_d(x_d)))}{\log(f_d(x_d))} \leq \frac{f_d(x_d) \log(2 \log(f_d(x_d) + o(1)))}{\log(f_d(x_d) + o(1))} \leq (1 + o(1)) \frac{\pi^2}{3e^7} \sqrt{d}.$$ 

Combining the above with the bounds $p \geq \frac{4}{3}$ from Lemma 8 we obtain the result. \hfill $\Box$

3. NUMERICS

Table 1 illustrates the phenomenon by giving the ratio  

$$\text{Ratio} = p/ \left( \frac{3e^7}{2\pi} \right)^2 \left( \frac{\log(|D_L|) \log(2 \log(|D_L|))}{\log \log(|D_L|)} \right)^2$$

for an example of a the Hilbert class field of a quadratic imaginary field of each class number less than 100 with large discriminant.

Note that in Table 1 we have $K = \mathbb{Q}(\sqrt{-d})$ and $|D_L| = d^{h_K}$.

REFERENCES

[1] Jeoung-Hwan Ahn and Soun-Hi Kwon, An explicit upper bound for the least prime ideal in the Chebotarev density theorem, preprint, arxiv.org/abs/1807.00508.

[2] Eric Bach and Jonathan Sorenson, Explicit bounds for primes in residue classes, Math. Comp. 65 (1996), no. 216, 1717–1735.

[3] Karim Belabas, Francisco Diaz y Diaz, and Eduardo Friedman, Small generators of the ideal class group, Math. Comp. 77 (2008), no. 262, 1185–1197.

[4] S. Chowla, Improvement of a theorem of linnik and walfisz, Proc. Lond. Math. Soc. s2-50 (1948), no. 1, 423–429.

[5] Andrew Granville and K Soundararaj, The distribution of values of $L(1, \chi_d)$, Geometric and Functional Analysis 13 (2003).

[6] Habiba Kadiri, Nathan Ng, and Peng-Jie Wong, The least prime number represented by a binary quadratic for $m$, arXiv e-prints (2018), arXiv:1803.03218.

[7] Asif Zaman, Bounding the least prime ideal in the Chebotarev density theorem, Funct. Approx. Comment. Math. 57 (2017), no. 1, 115–142.
Table 1. Examples of smallest split primes in Hilbert class fields of \(\mathbb{Q}(\sqrt{-d})\)

| \(h_K\) | \(d\) | \(p\) | Ratio | \(h_K\) | \(d\) | \(p\) | Ratio |
|--------|-----|-----|-----|--------|-----|-----|-----|
| 1      | 163 | 41  | 4.1557 | 34     | 189883 | 47491 | 2.2528 |
| 2      | 427 | 107 | 2.4287 | 35     | 210907 | 52727 | 2.3373 |
| 3      | 907 | 227 | 2.1188 | 36     | 217627 | 54409 | 2.2819 |
| 4      | 1555 | 389 | 1.9476 | 37     | 158923 | 39733 | 1.6620 |
| 5      | 2683 | 673 | 2.0276 | 38     | 289663 | 72493 | 2.6454 |
| 6      | 3763 | 941 | 1.9222 | 39     | 253507 | 63377 | 2.2500 |
| 7      | 5923 | 1481 | 2.1071 | 40    | 260947 | 65239 | 2.2034 |
| 8      | 6307 | 1579 | 1.7569 | 41    | 296587 | 74149 | 2.3513 |
| 9      | 10627 | 2657 | 2.1729 | 42    | 280267 | 70067 | 2.1445 |
| 10     | 13843 | 3461 | 2.2386 | 43    | 300787 | 75209 | 2.1838 |
| 11     | 15667 | 3917 | 2.0939 | 44    | 319867 | 79967 | 2.2079 |
| 12     | 17803 | 4451 | 1.9938 | 45    | 308323 | 77081 | 2.0542 |
| 13     | 20563 | 5147 | 1.9503 | 46    | 462883 | 115727 | 2.7990 |
| 14     | 30067 | 7517 | 2.3373 | 47    | 375523 | 93887 | 2.2489 |
| 15     | 34483 | 8623 | 2.3173 | 48    | 335203 | 83813 | 1.9638 |
| 16     | 31243 | 7817 | 1.9050 | 49    | 393187 | 98297 | 2.1693 |
| 17     | 37123 | 9281 | 1.9719 | 50    | 389467 | 97367 | 2.0743 |
| 18     | 48427 | 12107 | 2.2225 | 51    | 546067 | 136519 | 2.6772 |
| 19     | 38707 | 9677 | 1.6747 | 52    | 439147 | 109789 | 2.1422 |
| 20     | 58507 | 14627 | 2.1572 | 53    | 425107 | 106277 | 2.0124 |
| 21     | 61483 | 15373 | 2.0614 | 54    | 532123 | 133033 | 2.3604 |
| 22     | 85507 | 21377 | 2.5024 | 55    | 452083 | 113021 | 1.9839 |
| 23     | 90787 | 22697 | 2.4308 | 56    | 494323 | 123581 | 2.0737 |
| 24     | 111763 | 27941 | 2.6847 | 57    | 618883 | 153991 | 2.4279 |
| 25     | 93307 | 23327 | 2.1425 | 58    | 586987 | 146749 | 2.2565 |
| 26     | 103027 | 25759 | 2.1714 | 59    | 474307 | 118583 | 1.8204 |
| 27     | 103387 | 25847 | 2.0351 | 60    | 662803 | 165701 | 2.3566 |
| 28     | 126043 | 31511 | 2.2543 | 61    | 606643 | 151667 | 2.1185 |
| 29     | 166147 | 41539 | 2.6760 | 62    | 647707 | 161947 | 2.1768 |
| 30     | 134467 | 33617 | 2.1037 | 63    | 991027 | 247759 | 3.0550 |
| 31     | 133387 | 33347 | 1.9698 | 64    | 693067 | 173267 | 2.1783 |
| 32     | 164803 | 41201 | 2.2263 | 65    | 703123 | 175781 | 2.1443 |
| 33     | 222643 | 55661 | 2.7216 | 66    | 958483 | 239623 | 2.7278 |

E-mail address: andrew.fiori@uleth.ca

Mathematics and Computer Science, 4401 University Drive, University of Lethbridge, Lethbridge, Alberta, T1K 3M4