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. Moreover, certain conditions which would tend to violate GRH would actually imply stronger results (see Propositions 9 and 10). In the formula above, and throughout the paper, γ is the Euler-Macheroni constant.

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 $\mathcal{C}$ in $\Gamma(L/K)$, the Galois group of L/K, show that the smallest (in norm) unramified degree one prime $\mathfrak{p}$ of K for which the conjugacy class $\mathrm{Frob}_{\mathfrak{p}}$ is $\mathcal{C}$ 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 $N_{K/\mathbb{Q}}(\mathfrak{p}) < (\log(|D_L|))^{2+o(1)}$ conditionally on GRH (see [7]).
- Bach and Sorenson gave an explicit constant C so that $N_{K/\mathbb{Q}}(\mathfrak{p}) < C\left(\log(|D_L|)\right)^2$ conditionally on GRH (see [2]).
- Lagarias, Montgomery, and Odlyzko showed there is a constant A such that $N_{K/\mathbb{Q}}(\mathfrak{p}) < |D_L|^A$ (see [6]).
- Zaman showed $N_{K/\mathbb{Q}}(\mathfrak{p}) < |D_L|^{40}$ for D_L sufficiently large (see [10]).
- Kadiri, Ng and Wong improved this to $N_{K/\mathbb{Q}}(\mathfrak{p}) < |D_L|^{16}$ for D_L sufficiently large (see [5]).
- Ahn and Kwon showed $N_{K/\mathbb{Q}}(\mathfrak{p}) < |D_L|^{12577}$ for all L (see [1]).

In light of 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.

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.

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 $d = |\mathrm{disc}(K)|$, then the smallest prime p of $\mathbb{Q}$ which is a norm from $\mathcal{O}_K$ is at least $d/4$.*

Proof. We first 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 $\mathcal{O}_k \subset \frac{1}{2}\mathbb{Z} + \frac{\sqrt{-d}}{2}\mathbb{Z}$ we conclude that if the norm is a prime, then $y \geq \frac{1}{2}$, from which the result follows. □

Lemma 3. *Let $K = \mathbb{Q}(\sqrt{-d})$ where $d = |\mathrm{disc}(K)|$, 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. □

Lemma 4. *Let $K = \mathbb{Q}(\sqrt{-d})$ where $d = |\mathrm{disc}(K)|$, 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 $(p) = \mathfrak{p}_1\mathfrak{p}_1$ where both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are principal. 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. □

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

$$\log(|D_H|) = h_K \log(d)$$

where h_K is the class number of K and D_H is the discriminant of H.

This is follows immediately from the multiplicativity of the discriminant in towers.

We now remind the reader of key analytic results, both of which follow from the analytic class number formula

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

and bounds on $L(1, \chi_d)$. We shall only need the unconditional result.

Theorem 6 (GRH-conditional)**.** *Let $K = \mathbb{Q}(\sqrt{-d})$ where $d = |\mathrm{disc}(K)|$. The class number of K satisfies:*

$$h_K > (1 + o(1)) \frac{\pi\sqrt{d}}{12e^\gamma \log\log d}.$$

This was proven by Littlewood (see [8]).

Theorem 7 (Unconditional)**.** *There exists a family of quadratic imaginary fields $K = \mathbb{Q}(\sqrt{-d})$ where $d = |\mathrm{disc}(K)|$ such that for each we have that class number of K satisfies:*

$$h_K < (1 + o(1)) \frac{\pi\sqrt{d}}{6e^\gamma \log\log d}.$$

A result of this sort was originally proven by Littlewood conditional on the generalized Riemann hypothesis (see [8]), his result was proven unconditionally by Paley (see [9]) the version stated here follows from the work of Chowla (see [4]).

Proposition 8. *Suppose* $0 \le \epsilon < \frac{1}{2}$ *and* $d > 100$. *Let* $K = \mathbb{Q}(\sqrt{-d})$ *where* $d = |\mathrm{disc}(K)|$, *if the class number of* K *satisfies*

$$(1-\epsilon)\frac{\pi\sqrt{d}}{12e^{\gamma}\log\log d} < h_K < \frac{\pi\sqrt{d}}{6e^{\gamma}\log\log d}(1+\epsilon)$$

then the smallest prime p, *which splits completely in* H, *the Hilbert class field of* K *satisfies*

$$(1+\epsilon)^{-2}\left(\frac{3e^{\gamma}}{2\pi}\right)^2\left(\frac{\log(|D_H|)\log(2\log\log(|D_H|))}{\log\log(|D_H|)}\right)^2 < p.$$

Proof. We have by Lemma 4 that the smallest prime p which splits completely in H satisfies $d \le 4p$ and by Lemma 5 that $\log(|D_H|) = h_K \log(d)$. We conclude by using our assumed upper bound on h_K that

$$(\log(|D_H|))^2 < (1+\epsilon)^2\left(\frac{\pi}{6e^{\gamma}}\right)^2\left(\frac{\log d}{\log\log d}\right)^2 d.$$

We also have, using the assumed lower bound on h_K, that

$$\begin{aligned}\log\log(|D_H|) &= \log(h_K) + \log\log(d)\\ &> \frac{1}{2}\log(d) + \log\left(\frac{\pi}{12e^{\gamma}}\right) - \log\log\log d + \log(1-\epsilon) + \log\log(d)\end{aligned}$$

and thus conclude by the bound on ϵ and d that

$$2\log\log(|D_H|) > \log(d)$$

and consequently by the monotonicity of $x/\log(x)$ we have that

$$\frac{2\log\log(|D_H|)}{\log(2\log\log(|D_H|))} > \frac{\log(d)}{\log\log(d)}.$$

Combining these inequalities gives

$$(1+\epsilon)^{-2}\left(\frac{3e^{\gamma}}{2\pi}\right)^2\left(\frac{\log(|D_H|)\log(2\log\log(|D_H|))}{\log\log(|D_H|)}\right)^2 < p. \qquad \square$$

Remark. We note before proceeding that by Theorem 7 the hypotheses of the next two propositions being satisfied infinitely often would imply the failure of GRH. Moreover, both results tend to give stronger lower bounds than the previous proposition.

Proposition 9. *Let* $K = \mathbb{Q}(\sqrt{-d})$ *where* $d = |\mathrm{disc}(K)|$, *if the class number of* K *satisfies*

$$h_K < \frac{\pi\sqrt{d}}{6e^{\gamma}\log d}$$

then the smallest prime p *which splits completely in* H, *the Hilbert class field of* K *satisfies*

$$\left(\frac{3e^{\gamma}}{\pi}\right)^2(\log(|D_H|))^2 < p.$$

Proof. Proceeding as in Proposition 8 we have that

$$d < 4p, \qquad \log(|D_H|) = h_K\log(d), \qquad h_K < \frac{\pi\sqrt{d}}{6e^{\gamma}\log d}$$

and so may quickly conclude that

$$\log(|D_H|) < \frac{\pi\sqrt{d}}{6e^{\gamma}}$$

so that

$$\left(\frac{3e^{\gamma}}{\pi}\right)^2(\log(|D_H|))^2 < p. \qquad \square$$

Proposition 10. *Suppose $d > 100$ then Let $K = \mathbb{Q}(\sqrt{-d})$ where $d = |\mathrm{disc}(K)|$, if the class number of K satisfies*

$$h_K = \frac{\pi\sqrt{d}}{6e^\gamma(\log d)^\alpha(\log\log d)^{1-\alpha}}$$

for $0 \le \alpha \le 1$ then the smallest prime p which splits completely in H, the Hilbert class field of K satisfies

$$\left(1 + \frac{\log(\pi/6e^\gamma)}{\log\log(D_H)}\right)^{2-2\alpha}\left(\frac{3e^\gamma}{\pi}\right)^2\left(\frac{\log(2\log\log(|D_H|))}{2\log\log(|D_H|)}\right)^{2-2\alpha}(\log(|D_H|))^2 < p.$$

Proof. Proceeding as in Proposition 8 we have that

$$\log(|D_H|) = \frac{\pi\sqrt{d}}{6e^\gamma}\left(\frac{\log(d)}{\log\log(d)}\right)^{1-\alpha}$$

but then

$$\log\log(|D_H|) = \frac{1}{2}\log(d) + \log\left(\frac{\pi}{6e^\gamma}\right) + (1-\alpha)\big(\log\log(d) - \log\log\log(d)\big)$$

which gives, by the choice of $d > 100$, both that

$$\log\log(|D_H|) > \frac{1}{2}\left(1 + \frac{\log(\pi/6e^\gamma)}{\log(d)}\right)\log(d)$$

and that

$$\log(d) > \log\log(|D_H|).$$

As $\log(\pi/6e^\gamma)$ is negative, by combining the above we conclude that

$$2\log\log(|D_H|)\left(1 + \frac{\log(\pi/6e^\gamma)}{\log\log(|D_H|)}\right)^{-1} > \log(d).$$

Proceeding as in the previous two propositions we obtain

$$\left(1 + \frac{\log(\pi/6e^\gamma)}{\log\log(D_H)}\right)^{2-2\alpha}\left(\frac{3e^\gamma}{\pi}\right)^2\left(\frac{\log(2\log\log(|D_H|))}{2\log\log(|D_H|)}\right)^{2-2\alpha}(\log(|D_H|))^2 < p. \qquad \square$$

Proof of Theorem 1. It follows from Theorem 7 that there are infinitely many fields which satisfy the conditions of at least one of Propositions 8, 9, or 10 and hence we obtain infinitely many satisfying the weakest conclusion. When considering Proposition 8 we note that Theorem 7 allows ϵ to be taken to be a function which is $o(1)$ as d, and hence D_L go to infinity, as such we obtain the bound

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

for d which satisfy Proposition 8. The worst case bound from Proposition 10 is in the case $\alpha = 0$ in which case we obtain a bound

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

agreeing with the bound from Proposition 8. The bound from Proposition 9 is strictly stronger. $\square$

3. Numerics

Table 1 illustrates the phenomenon by giving the ratio

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

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 $K = \sqrt{-d}$ and $|D_L| = d^{h_K}$.

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	h_K	D	p	Ratio
1	163	41	4.1557	34	189883	47491	2.2528	67	652723	163181	1.9030
2	427	107	2.4287	35	210907	52727	2.3373	68	819163	204791	2.2546
3	907	227	2.1188	36	217627	54409	2.2819	69	888427	222107	2.3556
4	1555	389	1.9476	37	158923	39733	1.6620	70	811507	202877	2.1215
5	2683	673	2.0276	38	289963	72493	2.6454	71	909547	227387	2.2823
6	3763	941	1.9222	39	253507	63377	2.2500	72	947923	236981	2.3061
7	5923	1481	2.1071	40	260947	65239	2.2034	73	886867	221717	2.1227
8	6307	1579	1.7569	41	296587	74149	2.3513	74	951043	237763	2.2001
9	10627	2657	2.1729	42	280267	70067	2.1445	75	916507	229127	2.0792
10	13843	3461	2.2386	43	300787	75209	2.1838	76	1086187	271549	2.3521
11	15667	3917	2.0939	44	319867	79967	2.2079	77	1242763	310693	2.5821
12	17803	4451	1.9938	45	308323	77081	2.0542	78	1004347	251087	2.0958
13	20563	5147	1.9503	46	462883	115727	2.7990	79	1333963	333491	2.6208
14	30067	7517	2.3373	47	375523	93887	2.2489	80	1165483	291371	2.2775
15	34483	8623	2.3173	48	335203	83813	1.9638	81	1030723	257687	2.0011
16	31243	7817	1.9050	49	393187	98297	2.1693	82	1446547	361637	2.6277
17	37123	9281	1.9719	50	389467	97367	2.0743	83	1074907	268729	1.9851
18	48427	12107	2.2225	51	546067	136519	2.6772	84	1225387	306347	2.1765
19	38707	9677	1.6747	52	439147	109789	2.1422	85	1285747	321443	2.2210
20	58507	14627	2.1572	53	425107	106277	2.0124	86	1534723	383681	2.5366
21	61483	15373	2.0614	54	532123	133033	2.3604	87	1261747	315437	2.0941
22	85507	21377	2.5024	55	452083	113021	1.9839	88	1265587	316403	2.0564
23	90787	22697	2.4308	56	494323	123581	2.0737	89	1429387	357347	2.2395
24	111763	27941	2.6847	57	615883	153991	2.4279	90	1548523	387137	2.3529
25	93307	23327	2.1425	58	586987	146749	2.2565	91	1391083	347771	2.1002
26	103027	25759	2.1714	59	474307	118583	1.8204	92	1452067	363017	2.1371
27	103387	25847	2.0351	60	662803	165701	2.3566	93	1475203	368801	2.1244
28	126043	31511	2.2543	61	606643	151667	2.1185	94	1587763	396943	2.2212
29	166147	41539	2.6760	62	647707	161947	2.1768	95	1659067	414767	2.2638
30	134467	33617	2.1037	63	991027	247759	3.0559	96	1684027	421009	2.2501
31	133387	33347	1.9698	64	693067	173267	2.1783	97	1842523	460633	2.3882
32	164803	41201	2.2263	65	703123	175781	2.1443	98	2383747	595939	2.9359
33	222643	55661	2.7216	66	958483	239623	2.7278	99	1480627	370159	1.9012

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] Habiba Kadiri, Nathan Ng, and Peng-Jie Wong, *The least prime ideal in the chebotarev density theorem*, To Appear in Proc. Amer. Math. Soc.

[6] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), no. 3, 271–296.

[7] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, (1977), 409–464.

[8] J. E. Littlewood, *On the class-number of the corpus* $p(\sqrt{-k})$, Proc. Lond. Math. Soc. **s2-27** (1928), no. 1, 358–372.

[9] R. E. A. C. Paley, *A theorem on characters*, J. Lond. Math. **s1-7** (1932), no. 1, 28–32.

[10] Asif Zaman, *Bounding the least prime ideal in the Chebotarev density theorem*, Funct. Approx. Comment. Math. **57** (2017), no. 1, 115–142.

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

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