Algebra & Number Theory

Volume 13
2019
No. 9

Lower bounds for the least prime in Chebotarev

Andrew Fiori

msp

ALGEBRA AND NUMBER THEORY 13:9 (2019)
dx.doi.org/10.2140/ant.2019.13.2199

Lower bounds for the least prime in Chebotarev

Andrew Fiori

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 $\mathcal{C}$ 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 [Belabas et al. 2008]) where smaller is better. Some of the history of just how small we can get is summarized below:

- Lagarias and Odlyzko [1977] showed $N_{K/\mathbb{Q}}(\mathfrak{p}) < (\log(|D_L|))^{2+o(1)}$ conditionally on GRH.
- Bach and Sorenson [1996] gave an explicit constant C so that $N_{K/\mathbb{Q}}(\mathfrak{p}) < C(\log(|D_L|))^2$ conditionally on GRH.
- Lagarias, Montgomery, and Odlyzko [Lagarias et al. 1979] showed there is a constant A such that $N_{K/\mathbb{Q}}(\mathfrak{p}) < |D_L|^A$.

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.
MSC2010: primary 11R44; secondary 11R29.
Keywords: Chebotarev, class groups.

- Zaman [2017] showed $N_{K/\mathbb{Q}}(\mathfrak{p}) < |D_L|^{40}$ for D_L sufficiently large.
- Kadiri, Ng and Wong [Kadiri et al. 2019] improved this to $N_{K/\mathbb{Q}}(\mathfrak{p}) < |D_L|^{16}$ for D_L sufficiently large.
- Ahn and Kwon [2019] showed $N_{K/\mathbb{Q}}(\mathfrak{p}) < |D_L|^{12577}$ for all L.

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 [2018, Section 1.3] where some similar features of this family are remarked on in a different context.

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 $d = |\mathrm{disc}(K)|$, 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 $p \geq \frac{d}{4}$.*

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 $\mathcal{O}_k \subset \frac{1}{2}\mathbb{Z} + \frac{\sqrt{-d}}{2}\mathbb{Z}$ we conclude that if the norm is a prime, then $y \geq \frac{1}{2}$, from which it follows that if p is a norm then $p \geq \frac{d}{4}$. □

Lemma 3. *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 and $N_{K/\mathbb{Q}}(\mathfrak{p}_i) = (p)$. In particular, by the previous lemma $p \geq \frac{d}{4}$.*

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. □

Remark 4. Denote by χ_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 $d = |\mathrm{disc}(K)| > 16$, suppose that H is the Hilbert class field of K. Then*

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

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

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

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 $d = |\mathrm{disc}(K)|$ such that for χ_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 [1928] conditional on the generalized Riemann hypothesis, his result was proven unconditionally by Paley [1932] the version stated here follows from the work of Chowla [1949]. It is possible that the work of Granville and Soundararajan [2003] can further refine the constants in the above, and consequently those in Theorem 1.

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

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

and by Lemma 5 we have

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

Now because the function $y \mapsto y\log(2\log(y))/\log(y)$ 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

$$\begin{aligned}\frac{\log|D_L|\log(2\log\log|D_L|)}{\log\log|D_L|} &= \frac{f_d(x_d)\log(2\log(f_d(x_d)))}{\log(f_d(x_d))}\\ &\leq \frac{f_d\left(\frac{\pi^2}{6e^\gamma}+o(1)\right)\log\left(2\log\left(f_d\left(\frac{\pi^2}{6e^\gamma}+o(1)\right)\right)\right)}{\log\left(f_d\left(\frac{\pi^2}{6e^\gamma}+o(1)\right)\right)}\\ &\leq (1+o(1))\frac{\pi}{3e^\gamma}\sqrt{d}.\end{aligned}$$

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

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 $K = \mathbb{Q}(\sqrt{-d})$ and $|D_L| = d^{h_K}$.

References

[Ahn and Kwon 2019] J.-H. Ahn and S.-H. Kwon, "An explicit upper bound for the least prime ideal in the Chebotarev density theorem", *Ann. Inst. Fourier* (*Grenoble*) **69**:3 (2019), 1411–1458. Zbl

[Bach and Sorenson 1996] E. Bach and J. Sorenson, "Explicit bounds for primes in residue classes", *Math. Comp.* **65**:216 (1996), 1717–1735. MR Zbl

[Belabas et al. 2008] K. Belabas, F. Diaz y Diaz, and E. Friedman, "Small generators of the ideal class group", *Math. Comp.* **77**:262 (2008), 1185–1197. MR Zbl

[Chowla 1949] S. Chowla, "Improvement of a theorem of Linnik and Walfisz", *Proc. London Math. Soc.* (2) **50** (1949), 423–429. MR Zbl

[Granville and Soundararajan 2003] A. Granville and K. Soundararajan, "The distribution of values of $L(1, \chi_d)$", *Geom. Funct. Anal.* **13**:5 (2003), 992–1028. MR Zbl

[Kadiri et al. 2019] H. Kadiri, N. Ng, and P.-J. Wong, "The least prime ideal in the Chebotarev density theorem", *Proc. Amer. Math. Soc.* **147**:6 (2019), 2289–2303. MR Zbl

[Lagarias and Odlyzko 1977] J. C. Lagarias and A. M. Odlyzko, "Effective versions of the Chebotarev density theorem", pp. 409–464 in *Algebraic number fields: L-functions and Galois properties* (Durham, UK, 1975), edited by A. Fröhlich, Academic Press, London, 1977. MR Zbl

[Lagarias et al. 1979] 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**:3 (1979), 271–296. MR Zbl

[Littlewood 1928] J. E. Littlewood, "On the class-number of the corpus $P(\sqrt{-k})$", *Proc. London Math. Soc.* (2) **27**:1 (1928), 358–372. MR Zbl

[Paley 1932] R. E. A. C. Paley, "A theorem on characters", *J. London Math. Soc.* **7**:1 (1932), 28–32. MR Zbl

[Sardari 2018] N. T. Sardari, "The least prime number represented by a binary quadratic form", preprint, 2018. arXiv

[Zaman 2017] A. Zaman, "Bounding the least prime ideal in the Chebotarev density theorem", *Funct. Approx. Comment. Math.* **57**:1 (2017), 115–142. MR Zbl

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

Table 1. Examples of smallest split primes in Hilbert class fields of $\mathbb{Q}(\sqrt{-d})$.

Communicated by Andrew Granville
Received 2019-03-01 Revised 2019-05-08 Accepted 2019-06-27

andrew.fiori@uleth.ca *Department of Mathematics and Computer Science, University of Lethbridge, AB, Canada*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2019 is US $385/year for the electronic version, and $590/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 13 No. 9 2019

1937-0652(2019)13:9;1-4