Prime splitting on average in cubic number fields

Paul Pollack

Abstract. Let K be a degree 3 extension of $\mathbf{Q}$. We show that if one averages over all K, ordered by discriminant, then the least rational prime that does not split completely in K is

$$\sum_{r} \frac{r(5/6+1/r+1/r^2)}{1+1/r+1/r^2} \prod_{p<r} \frac{1/6}{1+1/p+1/p^2} = 2.1211027268\ldots,$$

where r runs over all rational primes. We also discuss the analogous question for other splitting types.

1. Introduction

For an odd prime p, let $n_2(p)$ denote the least quadratic nonresidue modulo p. Quite a bit of work has gone into showing that $n_2(p)$ can never be “too large”; on the generalized Riemann Hypothesis, Ankeny [**Ank52**] showed that $n_2(p) \ll (\log p)^2$, and by work of Bach [**Bac90**], one may take the implied constant equal to 2 here. But the sharpest upper bound known unconditionally, due to Burgess [**Bur57**], is that $n_2(p) \ll p^{\frac{1}{4\sqrt{e}}+\epsilon}$. While we cannot rule out that $n_2(p)$ is occasionally this large, the large sieve, as developed by Linnik, shows that $n_2(p)$ is usually much smaller. This enabled Erdős [**Erd61**] to prove that $n_2(p)$ has a finite mean value: In fact, as $x \to \infty$,

$$\frac{1}{\pi(x)} \sum_{2<p\leq x} n_2(p) \to \sum_{k=1}^{\infty} \frac{p_k}{2^k},$$

where p_k denotes the kth prime in increasing order.

We may view $n_2(p)$ as the least prime that does not split completely in the quadratic field of conductor p (equivalently, of discriminant $p^* := (-1)^{(p-1)/2}p$). Thus, Erdős's theorem can be interpreted as giving the average least non-split prime in a quadratic extension, where the average is taken over quadratic fields where the discriminant is a positive or negative rational prime. In [**Pol11**], the author obtained variants of this result (for both the split and inert cases) where the average is taken over *all* quadratic fields, ordered by absolute value of the discriminant.

For a prime $p \equiv 1 \pmod 3$, define $n_3(p)$ as the least cubic nonresidue modulo p. That $n_3(p)$ possesses a finite mean-value was shown by Elliott [**Ell68**]. (In fact, he showed the analogous result for $n_k(p)$ for each fixed k.) One can view $n_3(p)$ is the least prime that does not split completely in the cyclic cubic extension of $\mathbf{Q}$ of conductor p, and so Elliott's result admits a similar interpretation as Erdős's, but for the class of cyclic cubic extensions of prime conductor (i.e., cyclic cubic extensions of discriminant p^2). The goal of this note is to prove the following theorem, which gives the average least non-split prime over *all* cubic extensions of $\mathbf{Q}$, ordered by discriminant. In what follows, we write d_K for the discriminant of the number field $K/\mathbf{Q}$.

Theorem 1.1. *For a cubic number field K, let n_K denote the least rational prime which does not split completely in K. Then as $x \to \infty$,*

$$\frac{\sum_{|d_K| \le x} n_K}{\sum_{|d_K| \le x} 1} \to \sum_{r} \frac{r(5/6 + 1/r + 1/r^2)}{1 + 1/r + 1/r^2} \prod_{p<r} \frac{1/6}{1 + 1/p + 1/p^2} \quad \text{as } x \to \infty. \tag{1.1}$$

Here the left-hand sums are over all cubic fields K, up to isomorphism, for which $|d_K| \le x$, and the right-hand sum is over all primes r.

Remark 1.2. The numerical value of the right-hand sum is $2.1211027268\ldots$. As a reality check, we sampled fields with discriminant $\approx -10^{12}$. Using K. Belabas's `cubics` package (see [**Bel97, Bel04**]) and `PARI/GP`, we found that the average of n_K over fields with $|d_K - X| \le 250000$ is $2.1206494717\ldots$.

2. Proof of Theorem 1.1

The first ingredient in the proof is a now classical theorem of Davenport and Heilbronn [**DH71**]: As $x \to \infty$, the number of cubic fields K with $|d_K| \le x$ is $\sim \frac{x}{3\zeta(3)}$, as $x \to \infty$. The second is a recent theorem of Taniguchi and Thorne [**TT11**, Theorem 1.3] giving precise counts of cubic fields with specified local behavior. We need the following consequence of their (more general) result:

Proposition 2.1. *Let $x \ge 1$, and let $y = \frac{1}{50}\log x$. For each prime $p \le y$, we define a local factor c_p depending on the desired splitting type of p as follows:*

$$c_p := \begin{cases} 1/6 & \text{if } p \text{ is to split completely,} \\ 1/2 & \text{if } p \text{ is to split partially,} \\ 1/3 & \text{if } p \text{ is to be inert,} \\ 1/p & \text{if } p \text{ is to partially ramify,} \\ 1/p^2 & \text{if } p \text{ is to ramify completely.} \end{cases}$$

The number of cubic number fields K (up to isomorphism) with $|d_K| \le x$ and satisfying these conditions, is

$$\frac{1}{3\zeta(3)} \left(\prod_{p \le y} \frac{c_p}{1 + 1/p + 1/p^2} \right) x + O(x^{5/6}),$$

uniformly in the choice of the c_p.

If K is a cubic field with non-cyclic Galois group, then the splitting field of $K/\mathbf{Q}$ contains a unique quadratic subfield, called the *quadratic resolvent* of K. If K is cyclic, we adopt the convention that K has quadratic resolvent $\mathbf{Q}$; in both cases, the quadratic resolvent is $\mathbf{Q}(\sqrt{d_K})$. The next lemma provides an upper bound on the number of cubic fields with a given quadratic resolvent. It should be noted that Cohen and Morra [**CM11**] have asymptotic results for this problem for a *fixed* quadratic resolvent, but in our application we require some uniformity.

Lemma 2.2. *As $x \to \infty$, the number of cubic fields of discriminant $\le x$ with a prescribed quadratic resolvent L is at most $x^{5/6+o(1)}$, uniformly in L.*

Proof. Suppose that K has quadratic resolvent L and that $|d_K| \le x$. Then $d_K = f^2 d_L$ for some positive integer f. Clearly, $f \le x^{1/2}$. So the number of choices for d_K is also $\le x^{1/2}$. Ellenberg and Venkatesh [**EV07**] have shown that the number of cubic fields with discriminant D is $\ll_\epsilon D^{1/3+\epsilon}$, and so the lemma follows upon summing over the possibilities for $D = d_K$. □

To handle the contribution to the average from fields K for which n_K is large, we need two results. The first is a universal upper bound on n_K, due to Li [**Li11**]:

Proposition 2.3. *If K is a cubic field, then the least non-split prime in K is $\ll |d_K|^{1/7.39}$.*

As discussed by Li, it is much simpler to prove Proposition 2.3 with the larger exponent $\frac{1}{4\sqrt{e}} + \epsilon$, which would also suffice for our purposes.

The next result, in slightly stronger form, appears without proof in a paper of Duke and Kowalski [**DK00**] (for details, see the proof of Lemma 5.3 in [**Pol11**]). Baier [**Bai06**] has proved a somewhat stronger result, which would allow us to replace $2/A$ below by $1/(A-1)$, but we shall not need this.

Lemma 2.4. *Fix $A > 2$. The number of primitive Dirichlet characters χ of conductor $\leq x$ with $\chi(p) = 1$ for all primes $p \leq (\log x)^A$ is at most at most $x^{2/A+o(1)}$, as $x \to \infty$.*

Proof of Theorem 1.1. Set $y := \frac{1}{50}\log x$, and set $z := (\log x)^{100}$. Denoting n_K by r, we consider the contribution to the average from three ranges of n_K:

(i) $r \leq y$,
(ii) $y < r \leq z$,
(iii) $r > z$.

For the contribution of those r in range (i), Proposition 2.1 shows that

$$\sum_{\substack{|d_K| \leq x \\ n_K \leq y}} n_K = \frac{x}{3\zeta(3)} \sum_{r \leq y} \frac{r(5/6 + 1/r + 1/r^2}{1 + 1/r + 1/r^2)} \prod_{p<r} \frac{1/6}{1 + 1/p + 1/p^2} + O(x^{9/10})$$

$$= \left(\frac{1}{3\zeta(3)} + o(1)\right) x \sum_{r} \frac{r(5/6 + 1/r + 1/r^2)}{1 + 1/r + 1/r^2} \prod_{p<r} \frac{1/6}{1 + 1/p + 1/p^2}.$$

By the same proposition, the number of cubic fields K with $|d_K| \leq x$ for which every prime $p \leq y$ splits completely is

$$\ll x/6^{\pi(y)} + x^{5/6} \ll x/\exp\left(\frac{\log x}{30 \log\log x}\right),$$

and so

$$\sum_{\substack{|d_K| \leq x \\ y < n_K \leq z}} n_K \ll z \cdot x/\exp\left(\frac{\log x}{30 \log\log x}\right) \ll x/\exp\left(\frac{\log x}{31 \log\log x}\right),$$

say. In particular, this contribution is $o(x)$.

Finally, suppose $p > z$. Then every prime $p \leq z$ splits completely in the splitting field of K, and so also splits in the quadratic resolvent L of K. But the number of quadratic fields of discriminant $\leq x$ in which every prime $p \leq z$ splits is $\leq x^{1/50+o(1)}$. To see this, note that if L is a quadratic field with this property, then $\chi(\cdot) := \left(\frac{d_L}{\cdot}\right)$ is a primitive character of conductor $\leq x$ with $\chi(p) = 1$ for all $p \leq z$. The stated estimate now follows from Lemma 2.4. By Lemma 2.2, the number of corresponding cubic extensions K is at most

$$x^{1/50+5/6+o(1)}.$$

Finally, for each such K, Proposition (2.3) shows that $n_K \ll x^{1/7.39}$. So as $x \to \infty$,

$$\sum_{\substack{|d_K|\le x\\ n_K>z}} n_K \le x^{1/7.39+1/50+5/6+o(1)}.$$

The exponent here is < 0.99 for large x, and so this contribution is $o(x)$. Recalling that the denominator in (1.1) is $\sim \frac{1}{3\zeta(3)}x$, Theorem 1.1 follows. □

3. Concluding remarks

For each natural number k and each prime $p \equiv 1 \pmod{k}$, let $r_k(p)$ denote the least prime kth power residue modulo p. Elliott [**Ell71**] has shown that for each of $k = 2, 3$, and 4, the function $r_k(p)$ possesses a finite mean value. When $k = 3$, Elliott's result gives the average behavior of the least split prime in cubic extensions of prime conductor.

Motivated by Elliott's work, one might wonder if it is possible to obtain the average least split prime, taken over all cubic extensions of $\mathbf{Q}$ (ordered as in Theorem 1.1). Proposition 2.1 suggests that this mean value should exist and have value

$$\sum_{r} \frac{r/6}{1+1/r+1/r^2} \prod_{p<r} \frac{5/6+1/p+1/p^2}{1+1/p+1/p^2} = 19.7952216366\ldots.$$

More generally, for each splitting type of unramified primes (totally split, partially split, inert) the results of Taniguchi and Thorne yield what is surely the correct average value of the least such prime.

Unfortunately, the author has not succeeded in proving any of these conjectures. The difficulty lies in treating what is labeled range (iii) in the proof of Theorem 1.1, since analogues of Proposition 2.3 and Lemma 2.4 do not appear to be available. Some solace is found in noting that all such difficulties vanish if one assumes the Generalized Riemann Hypothesis, since in this case the least unramified prime p with a prescribed splitting type is $\ll \log^2|d_K|$ (see [**LO77**], [**LMO79**]), so that range (iii) contribues nothing at all!

Acknowledgements

The author thanks Mits Kobayashi for technical assistance with Karim Belabas's `cubics` package.

References

[Ank52] N. C. Ankeny, *The least quadratic non residue*, Ann. of Math. (2) **55** (1952), 65–72.

[Bac90] E. Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380.

[Bai06] S. Baier, *On the least n with $\chi(n) \neq 1$*, Q. J. Math. **57** (2006), no. 3, 279–283.

[Bel97] K. Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), no. 219, 1213–1237, software package `cubics` available from `http://www.math.u-bordeaux1.fr/~belabas/research/`.

[Bel04] ———, *On quadratic fields with large 3-rank*, Math. Comp. **73** (2004), no. 248, 2061–2074.

[Bur57] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika **4** (1957), 106–112.

[CM11] H. Cohen and A. Morra, *Counting cubic extensions with given quadratic resolvent*, J. Algebra **325** (2011), 461–478.

[DH71] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420.

[DK00] W. Duke and E. Kowalski, *A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations*, Invent. Math. **139** (2000), no. 1, 1–39.

[Ell68] P. D. T. A. Elliott, *A problem of Erdős concerning power residue sums*, Acta Arith. **13** (1967/1968), 131–149.

[Ell71] ______, *The least prime k-th-power residue*, J. London Math. Soc. (2) **3** (1971), 205–210.

[Erd61] P. Erdős, *Remarks on number theory. I*, Mat. Lapok **12** (1961), 10–17 (Hungarian).

[EV07] J. S. Ellenberg and A. Venkatesh, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. IMRN (2007), no. 1, Art. ID rnm002, 18.

[Li11] X. Li, *The smallest prime that does not split completely in a number field*, Algebra and Number Theory (2011), to appear.

[LMO79] 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.

[LO77] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 409–464.

[Pol11] P. Pollack, *The average least quadratic nonresidue modulo m and other variations on a theme of Erdős*, submitted.

[TT11] T. Taniguchi and F. Thorne, *Secondary terms in counting functions for cubic fields*, submitted.

University of British Columbia, Department of Mathematics, Room 121, 1984 Mathematics Road, Vancouver, BC Canada V6T 1Z2

E-mail address: gerg@math.ubc.ca

E-mail address: pollack@math.ubc.ca