

Math 286X: Arithmetic Statistics

Spring 2020

Some ideas for final papers

Here are some ideas for the **10–15 page** final papers (in arbitrary order). You are of course more than welcome to come up with your own topics!

1. *Asymptotics for regulator times class number:* We proved in class that

$$\sum_{\substack{K \text{ imaginary quadratic} \\ 0 < -D_K \leq T}} h_K \sim C \cdot T^{3/2}.$$

A somewhat similar proof (where R_K is “the size” of the stabilizer) should show that

$$\sum_{\substack{K \text{ real quadratic} \\ 0 < D_K \leq T}} R_K h_K \sim C' \cdot T^{3/2}.$$

(I haven’t checked whether this actually works, though! It might be too difficult for a final paper.) The (presumably more difficult) case of cubic number fields was treated using similar methods in Wilson’s thesis [Wil13, section 2].

2. *Lattice reduction theory:* We’ve discussed Minkowski reduced lattice bases and will discuss Hermite reduced lattice bases. However, there are many more notions of reduced bases. Most famously, LLL (Lenstra–Lenstra–Lovász) reduced bases can be computed in polynomial time. (This has plenty of applications to computational number theory and CS.) The original reference is [LLL82], but you can also find more modern treatments online.
3. *Siegel’s second finiteness theorem:* We’ve seen in class that the set of Minkowski reduced bases in dimension two is described by finitely many inequalities ($|b_1| \leq |b_2|$ and $2|b_1 \cdot b_2| \leq |b_1|^2$). The same holds in any dimension. An explanation of the proof and some more examples would be nice. A reference is [Sie89, chapter III, mostly lectures XI–XIV].

4. *Squarefree sieve using the ABC conjecture:* Granville showed in [Gra98] that the ABC conjecture implies that for $f(X) \in \mathbb{Z}[X]$ of any degree,

$$\mathbb{P}(f(x) \text{ squarefree} \mid x \in \mathbb{Z}) = \prod_p \mathbb{P}(f(x) \not\equiv 0 \pmod{p^2} \mid x \in \mathbb{Z}).$$

This is proven using so-called *Belyi functions*. (Reading the literature on Belyi functions might require familiarity with basic algebraic geometry.)

5. *Computing number fields:* We've computed upper and lower bounds for the number of number fields K of degree n with $|D_K| \leq T$. How can you find all of them? A reference is [Coh00, chapter 9].
6. *Probability that a root of a random polynomial generates its ring of integers:* In [ABZ07], the authors conjecture that a root of a random monic polynomial $f(X) \in \mathbb{Z}[X]$ (ordered by maximum coefficient) generates the ring of integers of $K = \mathbb{Q}[X]/f(X)$ with probability $\zeta(2)^{-1}$. This was later proven in [BSW16] (ordering $f(X)$ by height). The latter proof is rather involved, but the heuristic explanation given in [ABZ07] is more accessible (and certainly sufficient for a final project).
7. *Artin's primitive root conjecture:* (topic pointed out to me by Alexandr Petrov) Fix some integer $a \in \mathbb{Z}$. For a random prime number p , what is the probability that $a \pmod{p}$ generates \mathbb{F}_p^\times (i.e., a is a primitive root modulo p)? Using the Chebotarev density theorem, a careless sieve provides a (conjectural) answer. M. Ram. Murty [Mur88] has written a nice exposition on the topic. A thorough explanation for the conjecture and an upper bound for the probability (and maybe a short sketch of the proof of one of the known results) would be nice.
8. *Ehrhart polynomials:* Let $P \subset \mathbb{R}^n$ be a polytope whose vertices have integer coordinates. For any positive integer T , let $f(T) = \#(T \cdot P \cap \mathbb{Z}^n)$. It turns out that $f(T)$ is given by a polynomial with rational coefficients. (Widmer's theorem tells us that the leading term is $\text{vol}(P) \cdot T^n$.)

References

- [ABZ07] Avner Ash, Jos Brakenhoff, and Theodore Zarrabi. “Equality of polynomial and field discriminants”. In: *Experiment. Math.* 16.3 (2007), pp. 367–374. ISSN: 1058-6458. URL: <http://projecteuclid.org.ezp-prod1.hul.harvard.edu/euclid.em/1204928536>.
- [BSW16] Manjul Bhargava, Arul Shankar, and Xiaoheng Wang. *Squarefree values of polynomial discriminants I*. 2016. arXiv: 1611.09806 [math.NT].
- [Coh00] Henri Cohen. *Advanced topics in computational number theory*. Vol. 193. Graduate Texts in Mathematics. Springer-Verlag, New York, 2000, pp. xvi+578. ISBN: 0-387-98727-4. DOI: 10.1007/978-1-4419-8489-0. URL: <https://doi-org.ezp-prod1.hul.harvard.edu/10.1007/978-1-4419-8489-0>.
- [Gra98] Andrew Granville. “*ABC* allows us to count squarefrees”. In: *Internat. Math. Res. Notices* 19 (1998), pp. 991–1009. ISSN: 1073-7928. DOI: 10.1155/S1073792898000592. URL: <https://doi-org.ezp-prod1.hul.harvard.edu/10.1155/S1073792898000592>.
- [LLL82] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. “Factoring polynomials with rational coefficients”. In: *Math. Ann.* 261.4 (1982), pp. 515–534. ISSN: 0025-5831. DOI: 10.1007/BF01457454. URL: <https://doi.org/10.1007/BF01457454>.
- [Mur88] M. Ram Murty. “Artin’s conjecture for primitive roots”. In: *Math. Intelligencer* 10.4 (1988), pp. 59–67. ISSN: 0343-6993. DOI: 10.1007/BF03023749. URL: <https://doi-org.ezp-prod1.hul.harvard.edu/10.1007/BF03023749>.
- [Sie89] Carl Ludwig Siegel. *Lectures on the geometry of numbers*. Notes by B. Friedman, Rewritten by Komaravolu Chandrasekharan with the assistance of Rudolf Suter, With a preface by Chandrasekharan. Springer-Verlag, Berlin, 1989, pp. x+160. ISBN: 3-540-50629-2. DOI: 10.1007/978-3-662-08287-4. URL: <https://doi-org.ezp-prod1.hul.harvard.edu/10.1007/978-3-662-08287-4>.
- [Wil13] Kevin H. Wilson. *Three perspectives on n points in $P(n-2)$* . Thesis (Ph.D.)—Princeton University. ProQuest LLC, Ann Arbor, MI, 2013, p. 239. ISBN: 978-1267-92602-9. URL: http://gateway.proquest.com.ezp-prod1.hul.harvard.edu/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx

dissertation&res_dat=xri:pqm&rft_dat=xri:pqdiss:
3553265.