Math 514ab: Algebraic Number Theory / 2025–26
Project topic suggestions

Edits 11/19/25 in blue.
This is just a list of suggestions, varying in sophistication and required background, and in no particular order. Feel free to choose your own topic — come discuss it with me. Plan on a short writeup (7–15 pages, say) and give a short presentation (half of a 75min class, say, though you can go longer) during one of the last classes in early December or in the spring semester.
Consult at least two references. (Don't choose a topic you already happen to know well!)

(1) **The different ideal:** AKLB setting. The different is an ideal $\mathfrak{D}(B/A)$ of B refining the discriminant ideal $\Delta(B/A)$ of A. A prime $\mathcal{P}$ of B lying over $\mathfrak{p}$ in A divides $\mathfrak{D}(B/A)$ if and only if $e(\mathcal{P}/\mathfrak{p}) > 1$. There's also some control over the power of $\mathcal{P}$ dividing $\mathfrak{D}(B/A)$ depending on the ramification.

- $K/\mathbb{Q}$: See [Mar18], exercises 33–39 in Chapter 3.
- Classic reference: Chapter III of [Lan86].
- $K/\mathbb{Q}$ again: see Keith Conrad's blurb "The Different Ideal".
- Another writeup: Andrew Sutherland's lecture notes.
- Amusing aside: you can use the different ideal to get an alternate proof of Stickelberger's theorem, apparently due to user Tim.E on MathOverflow: https://math.stackexchange.com/a/2419398.

(2) **Dirichlet's theorem on primes in arithmetic progression:** Dirichlet's theorem, the inaugural result of modern analytic number theory, states that if $m \geq 1$ is a positive integer and a is relatively prime to m, then there are infinitely many primes congruent to a modulo m, and in fact the *Dirichlet density* of all such primes is $\frac{1}{\varphi(m)}$.

- We will cover this theorem in class, so definitely come talk to me about timing of your presentation.
- The classic reference (for my generation at least) is the last chapter of [Ser73].
- Marcus [Mar18] is playing with the same circle of ideas in Chapter 7, though surprisingly I don't see a complete proof of Dirichlet's theorem in the exercises.
- Exercise 12 of [Mar18, Chapter 7] gives a proof of the *Frobenius density theorem*, of which the Chebotarev density theorem (which reduces to Dirichlet's theorem for cyclotomic extensions of $\mathbb{Q}$) is a refinement.
- For comparison, see Keith Conrad's blurb on the limits of Euclid-style proofs of the infinitude of primes congruent to a modulo m.

(3) **Cohen-Lenstra heuristics:** These heuristics are a set of conjectures in arithmetic statistics describing the distribution of ideal classes in number fields, initially formulated for quadratic fields, though there is a variety of extensions, to number fields and to function fields.

- I gave the briefest of introductions to this story in class on 10/23/25.
- Start with Cohen–Lenstra's original paper: [CL84].
- Generalizations to other extensions of $\mathbb{Q}$: Cohen–Martinet [CM90, CM87], possible corrections by Bartel–Lenstra [BL20].

- Translations to function fields, where at least some versions of the conjectures are proved! [EVW16].

(4) **Herbrand's theorem:** Herbrand's theorem is a refinement of one part of Kummer's criterion: that an odd prime p is irregular if and only if p divides the numerator of the Bernoulli numbers $B_2, B_4, B_6, \ldots, B_{p-3}$. Namely, let $K = \mathbb{Q}(\mu_p)$, and let $A = C(K)[p]$ be the p-torsion part of the class group of K, written additively. (Here $\mu_p = \{1, \zeta_p, \ldots, \zeta_p^{p-1}\}$ is the set of p^{th} roots of 1.) Then A is an $\mathbb{F}_p$-vector space; note that p is a regular prime if and only if $A = 0$. The abelian group $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ is canonically isomorphic to $\mathbb{F}_p^\times$, with the isomorphism ω sending $g \in \Delta$ to $\omega(g) = b \in \mathbb{F}_p^\times$ if $g(\zeta) = \zeta^b$ for any $\zeta \in \mu_p$. One can show that Δ acts on A, and the action decomposes A into a direct sum of eigenspaces for characters $\Delta \to \mathbb{F}_p^\times$, which are all powers of ω:

$$A = \bigoplus_{k \bmod p-1} A(\omega^k), \qquad \text{where} \qquad A(\omega^k) = \{a \in A : g(a) = \omega^k(g)\, a \text{ for all } g \in \Delta\}.$$

Herbrand's theorem [Her32] asserts that, for $2 \le k \le p-3$ even, if $A(\omega^{1-k}) \neq 0$ then $p \mid B_k$. The proof uses Stickelberger's theorem about the action of a certain element of the group algebra of Δ on A. The converse was proved by Ribet [Rib76] using congruences between modular forms.

- Classic reference is [Was97, Theorem 6.17].
- Alternative: [Lan90, Corollary 3].
- This writeup by Carl Wang-Erickson focuses on Ribet's converse theorem, but provides a nice context for the story as well as a number of references. In particular, Appendix A.1 outlines a proof of the other, analytic, direction of Kummer's original criterion (that is, the direction refined by Ribet) in modern language; unpacking, understanding, and completing this argument could be a project in its own right. See also [Was97, Theorem 5.34].

(5) **Genus theory:** Genus theory, first studied by Gauss in the context of quadratic forms, can be used to describe the 2-torsion part of the class group of an imaginary quadratic field. Canonical reference in modern language is [Cox13, §3, 5, 6], especially Theorem 6.1.

(6) **Why is $e^{\pi\sqrt{163}}$ close to an integer?:** Indeed,

$$\begin{aligned} e^{\pi\sqrt{163}} &\approx 262537412640768743.999999999977262\ldots \\ &\approx 640320^3 + 744 - (2.274\ldots) \times 10^{-12}. \end{aligned}$$

It's not a coincidence that 163 is the biggest absolute-value discriminant of a quadratic imaginary field of class number 1. This connection is explained by the theory of *complex multiplication*, which in particular gives an explicit way of realizing the *Hilbert class field*[(i)] of a quadratic imaginary field.

[(i)] The Hilbert class field of a totally complex number field K is the maximal abelian everywhere unramified extension H/K. ~~Such an extension is automatically Galois (why?);~~ Class field theory tells you that $\mathrm{Gal}(H/K)$

Best for those who know a little bit about elliptic curves. Classic reference is [Sil94, Chapter II], especially example 6.2.1. See also [Cox13, Chapter III].

(7) **Continued fraction expansion for $\sqrt{d}$ and Pell's equation:** Let $d > 0$ be squarefree. The goal is to (limn the boundaries of and) understand the proof of the following statement: every unit $u = A + B\sqrt{d}$ of $\mathbb{Q}(\sqrt{d})$ with $A, B > 0$ can be found with $\frac{A}{B}$ among the convergents of the continued fraction for $\sqrt{d}$, as well as some expectations for how far you have to go to find a fundamental unit.

- I outlined quite a bit of this story in lecture on 11/4/25 and 11/6/25.
- Classic reference: Chapter X of [HW60].
- Short book by Khinchin: [Khi64].
- Super magic box reference: Course notes of Evan Dummit. (The super magic box is a bookkeeping device for computing convergents to $\sqrt{d}$, which I learned about as a counselor at the PROMYS program.)

(8) **Kronecker-Weber:** The Kronecker-Weber theorem states that any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension. We will eventually prove this as a consequence of the statements of global class field theory, but one can give a classical proof directly using what we know about factorization of prime ideals in number field extensions (so before the geometry of numbers unit of our course). See, for example, [Mar18], exercises 29–36 of chapter 4.

To come up with ideas for other topics, see, for example, the books in the bibliography below (especially [Cox13]), Keith Conrad's blurbs on algebraic number theory, or the many exercises of [Mar18]. One possibility is Kummer's full proof of Fermat's Last Theorem for regular primes, including Kummer's lemma about units of $\mathbb{Q}(\mu_p)$ that are congruent to integers modulo p being p^{th} powers in the regular case; see K.C.'s two blurbs on this topic as well as [Was97, Theorem 5.36]. Another possibility is understanding orders in number fields, perhaps from an algorithmic perspective: start with K.C.'s blurb on conductors and [Coh93].

References

[BL20] Alex Bartel and Hendrik W. Lenstra, Jr. On class groups of random number fields. *Proc. London Math. Soc.*, 121(3):927–953, 2020.

[CL84] H. Cohen and H.W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983*, volume 1068 of *Lecture Notes in Mathematics*, pages 33–62. Springer, 1984.

[CM87] H. Cohen and J. Martinet. Class groups of number fields: Numerical heuristics. *Mathematics of computation*, 48(177):123–137, January 1987.

[CM90] H. Cohen and J. Martinet. Étude heuristique des groupes de classes des corps de nombres. *Journal für die reine und angewandte Mathematik*, 404:39–76, 1990.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer, 1993.

[Cox13] David A. Cox. *Primes of the form x^2+ny^2: Fermat, class field theory, and complex multiplication.* Pure and Applied Mathematics (Hoboken). Wiley & Sons, second edition, 2013.

is canonically isomorphic to the class group $C(K)$, with $\text{Frob}_{\mathfrak{p}} \in \text{Gal}(H/K)$ corresponding to the ideal class $[\mathfrak{p}]$ for any prime $\mathfrak{p}$ of K.

[EVW16] Jordan S. Ellenberg, Akshay Venkatesh, and Craig Westerland. Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields. *Annals of Mathematics*, 183:729–786, 2016.

[Her32] Jacques Herbrand. Sur les classes des corps circulaires. *J. Math. Pures et Appliquées*, 9(11):417–441, 1932.

[HW60] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Clarendon Press: Oxford University Press, fourth edition, 1960.

[Khi64] A. Khinchin. *Continued Fractions*. University of Chicago Press, 1964.

[Lan86] Serge Lang. *Algebraic number theory*. Springer-Verlag, New York, 1986.

[Lan90] Serge Lang. *Cyclotomic Fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, combined second edition, 1990.

[Mar18] Daniel A. Marcus. *Number Fields*. Universitext. Springer, second edition, 2018.

[Rib76] Kenneth A. Ribet. A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$. *Inventiones Math.*, 34:151–162, 1976.

[Ser73] J-P. Serre. *A course in arithmetic*, volume 7 of *GTM*. Springer, 1973.

[Sil94] Joseph Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.