Math 223b: Algebraic Number Theory

Spring 2021

Some ideas for final papers

Here are some ideas for the 7–10 page final papers. You are of course more than welcome to come up with your own topics!

1. *Tate modules and the Weil pairing:* Since $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$, we have $\varprojlim_{k\to\infty} E[l^k] \cong (\mathbb{Z}_l)^2$. This is called the Tate module of E. An isogeny between elliptic curves induces a map of Tate modules, which can be represented by a 2×2-matrix with entries in $\mathbb{Z}_l$. It encodes a lot of useful information: For example, the degree of the isogeny is the determinant of this matrix. (See for example Chapters III.7 and III.8 in [Sil09].)

2. *Elliptic curves over $\mathbb{C}$:* An elliptic curve over $\mathbb{C}$ is (both analytically and as a group) isomorphic to $\mathbb{C}/\Lambda$ for a lattice $\Lambda \subset \mathbb{C}$ of rank 2. One can for example easily see the endomorphism ring of an elliptic curve from the lattice Λ. (See for example Chapter 2.2 in [ST15] or Chapter VI in [Sil09].)

3. *Complex multiplication:* In fall, we very explicitly constructed the maximal abelian extension K^{ab} of a field K when K is a local field or $K = \mathbb{Q}$. The case of general number fields is more difficult. The theory of complex multiplication provides a way to construct K^{ab} when K is a quadratic imaginary number fields. This involves looking at particular elliptic curves associated to K. (*Kronecker's Jugendtraum*) See for example [Cox13] or [67, Chapter XIII] or [ST15, Chapter 6] or [Sil94, Chapter II].

4. *Abelian varieties over $\mathbb{C}$:* Any abelian variety is isomorphic to $\mathbb{C}^g/\Lambda$ for a lattice $\Lambda \subset \mathbb{C}^g$ of rank $2g$. However, not every lattice arises from an abelian variety. A necessary and sufficient criterion is that there is a positive definite Hermitian form $\langle \cdot, \cdot \rangle$ on $\mathbb{C}^g$ with $\langle a, b \rangle \in \mathbb{Z}$ for all $a, b \in \Lambda$. There's also a nice interpretation of the Jacobian of a curve. This topic requires good knowledge of complex analysis and the theory of Riemann surfaces. (See for example Chapter I.2 in [Mil08] for a very short introduction, and then [Mur93].)

5. *The Nagell–Lutz theorem:* Roughly speaking, torsion points on elliptic curves have integer coordinates. (See for example Chapter 2 in [ST15].)

6. *The Bombieri–Lang conjecture:* This is a generalization of Faltings's theorem on curves of genus $g \geqslant 2$ to higher dimensional varieties. (There's a nice account and an example application on Terence Tao's blog: [Tao14])

7. *Elliptic curve factorization:* Elliptic curves can be used to factor integers. (See for example Chapter XI.2 in [Sil09].)

References

[67] *Algebraic number theory*. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press, London; Thompson Book Co., Inc., Washington, D.C., 1967, pp. xviii+366.

[Cox13] David A. Cox. *Primes of the form $x^2 + ny^2$*. Second. Pure and Applied Mathematics (Hoboken). Fermat, class field theory, and complex multiplication. John Wiley & Sons, Inc., Hoboken, NJ, 2013, pp. xviii+356. ISBN: 978-1-118-39018-4. DOI: 10.1002/9781118400722. URL: https://doi-org.ezp-prod1.hul.harvard.edu/10.1002/9781118400722.

[Mil08] James S. Milne. *Abelian Varieties (v2.00)*. Available at www.jmilne.org/math/. 2008.

[Mur93] V. Kumar Murty. *Introduction to abelian varieties*. Vol. 3. CRM Monograph Series. American Mathematical Society, Providence, RI, 1993, pp. xiv+112. ISBN: 0-8218-6995-7. DOI: 10.1090/crmm/003. URL: https://doi-org.ezp-prod1.hul.harvard.edu/10.1090/crmm/003.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6. URL: https://doi-org.ezp-prod1.hul.harvard.edu/10.1007/978-0-387-09494-6.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994, pp. xiv+525. ISBN: 0-387-94328-5. DOI: 10.1007/978-1-4612-0851-8. URL: https://doi-org.ezp-prod1.hul.harvard.edu/10.1007/978-1-4612-0851-8.

[ST15] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves*. Second. Undergraduate Texts in Mathematics. Springer, Cham, 2015, pp. xxii+332. ISBN: 978-3-319-18587-3; 978-3-319-18588-0. DOI: 10.1007/978-3-319-18588-0. URL: https://doi-org.ezp-prod1.hul.harvard.edu/10.1007/978-3-319-18588-0.

[Tao14] Terence Tao. *The Erdos-Ulam problem, varieties of general type, and the Bombieri-Lang conjecture*. Dec. 2014. URL: https://terrytao.wordpress.com/2014/12/20/the-erdos-ulam-problem-varieties-of-general-type-and-the-bombieri-lang-conjecture/.