MATH 115: ELLIPTIC CURVES
POSSIBLE FINAL PROJECTS

(1) Dummit has shown that the number of vertices in a bicolored Steiner triple system are counted by the number of points on an elliptic curve over a finite field, but this proof is not bijective. Explain the count and try to make this proof bijective.

(2) An elliptic curve over $\mathbb{Q}$ has a minimal Weierstrass equation, but this equation may not be the equation with the smallest coefficients. Explain this, give some examples, and try to find an algorithm (*reduction theory*) which gives an equation requiring the fewest number of bits.

(3) For an elliptic curve E over $\mathbb{Q}$, explain the (weak or strong) Birch–Swinnerton-Dyer conjecture where $r_E = \mathrm{rk}(E(\mathbb{Q}))$ is the rank of $E(\mathbb{Q})$, and investigate it by examples.

(4) Explain the work of Bhargava–Shankar, giving the expected size of n-Selmer groups for $n = 2, 3, 4, 5$. For $n = 3$, related their work to 3×3 Rubik's cubes and plane cubic curves.

(5) What is a tropical elliptic curve, and how do you compute its j-invariant?

(6) What is the congruent number problem? What is its conjectural resolution, using the arithmetic of elliptic curves?

(7) Define the Tate–Shafarevich group $Ш(E)$ of an elliptic curve E over $\mathbb{Q}$. In what ways is $Ш(E)$ like a class group (of an imaginary quadratic field)?

(8) If E is an elliptic curve over $\mathbb{Q}$ of rank 1, then there is a point $P_K \in E(\mathbb{Q})$, called a *Heegner point*, defined on E for certain imaginary quadratic extensions K of $\mathbb{Q}$. Define the Heegner point and compute it in some examples.

(9) Consider the elliptic curves over $\mathbb{Q}$ of rank 1. What is the probability that the generator lies on the real connected component of the identity?

(10) Let E be an elliptic curve over an imaginary quadratic field K of rank 1, generated by P and with torsion group $T = E(K)_{\mathrm{tors}}$. Let $\phi : E \to E'$ be the isogeny with kernel $\ker \phi = T$. Let $L = K(\phi^{-1}(P))$ be the extension of K obtained by adjoining all points $P \in E(\overline{K})$ such that $\phi(P') = P$. Then L/K is an abelian extension with Galois group a subgroup of T. Under what circumstances is L Galois not just over K, but Galois over $\mathbb{Q}$?

(11) Explain the Shimura–Taniyama conjecture, relating Hilbert modular forms to elliptic curves over totally real fields. Add some further matches to the LMFDB for fields of degree greater than or equal to 4.

(12) Take the tables of Hilbert modular forms over totally real quartic and quintic fields and see if there are any further elliptic curves with *sporadic* torsion subgroups.

(13) Explain Lenstra's algorithm for factoring integers using the group law on an elliptic curve.

(14) Explain Poonen's argument using elliptic divisibility sequences that gives a negative answer to Hilbert's tenth problem for $\mathbb{Z}[S^{-1}]$ where S is a set of primes of relative density 1.

Date: May 5, 2016.

(15) Park–Poonen–Voight–Wood give heuristics that model the arithmetic of elliptic curves in terms of random matrices. Explain this heuristic, and do some numerical experiments investigating their heuristic. Does this heuristic extend to directly model elliptic curves of higher rank?

(16) Deninger suggests: There are similarities between the distributions of spacings of zeroes of L-functions and those of the eigenvalues of hermitian random matrices. Is it clear that these analogies persist for ensembles of integral skew symmetric matrices? For example, one might also look at the statistics of the smallest non-real zero vis-à-vis the smallest non-zero eigenvalue.

(17) The Edwards model for elliptic curves is more efficient for arithmetic on an elliptic curve over a finite field. Explain the group law and discuss possible extensions to genus 2.

(18) Sylvester's conjecture predicts when the equation $x^3 + y^3 = p$ has a solution with $x, y \in \mathbb{Q}$ for primes p. Explain this conjecture and its relationship to the arithmetic of elliptic curves.

(19) If E is an elliptic curve over $\mathbb{Q}$, and p is an odd prime, then there is an injective map $E(\mathbb{Q})_{\text{tors}} \hookrightarrow E(\mathbb{F}_p)$. Does there exist $N \in \mathbb{Z}_{>0}$ such that $\#E(\mathbb{Q})_{\text{tors}} = \gcd(\#E(\mathbb{F}_p))_{p \leq N}$?

(20) Describe equations for elliptic curves embedded using the Riemann–Roch space $\mathscr{L}(n\infty)$ for small values of n (*elliptic normal curves* in $\mathbb{P}^{n-1}$). What structure can you find in these equations?

(21) Mestre and Nagao describe explicit procedures for producing elliptic curves of large rank over $\mathbb{Q}$. Explain this construction and try to extend it.

(22) Elliptic curves equipped with *fractional points* give rise to different and useful equations and models via a Riemann–Roch computation similar to Weierstrass equations, following Voight–Zureick-Brown. Discuss these and give an algorithm to compute the models given a fractional divisor.

(23) Schoof provides an algorithm to count points on an elliptic curve modulo p. Explain this algorithm, and the extensions due to Elkies and Atkin. Now suppose that E is an elliptic curve which has bad reduction modulo p but good reduction modulo p^2. Can you extend Schoof's algorithm to count points on E over $\mathbb{Z}/p^2\mathbb{Z}$?

(24) Bober and Spicer have given methods for (conjecturally) bounding the rank of an elliptic curve using an explicit sum involving the zeros of its L-function. Explain how this works and try to extend this method by predicting and modeling any low-lying zeros.

(25) Question of Brian Conrad: among ordinary elliptic curves over finite fields:
   (a) When is the endomorphism ring of an elliptic curve a maximal order?
   (b) When is the subring generated by Frobenius the entire endomorphism ring of the elliptic curve?
   (c) When is the subring generated by Frobenius a maximal order?

   "When" is supposed to be in some precise statistical sense–you could either consider all ordinary curves over a fixed $\mathbb{F}_q$, and then let $q \to \infty$; or take a fixed elliptic curve over $\mathbb{Q}$ and let $p \to \infty$. If you know the answers to (i) and (ii), you know the answer to (iii), but an answer to any one of them would be interesting.