18.783 Elliptic Curves
Course Outline, Spring 2022

Below is the sequence of topics planned for the course. Each corresponds to roughly a week of lectures (three hours), but some will be slightly less.

1. **Introduction**
   elliptic curves, the group law, Weierstrass and Edwards equations.
2. **Efficient computation**
   integer arithmetic, finite field arithmetic, root-finding, polynomial factorization.
3. **Isogenies and endomorphisms**
   the Frobenius endomorphism, division polynomials, Hasse's theorem.
4. **Elliptic curves over $\mathbb{F}_q$**
   point counting, baby-steps giant-steps, Schoof's algorithm.
5. **The discrete logarithm problem**
   ECEDH, Pollard rho, Pohlig-Hellman, generic lower bounds, index calculus.
6. **Integer factorization and primality proving**
   Lenstra ECM, Goldwasser-Killian ECPP, Montgomery curves.
7. **Endomorphism rings**
   the dual isogeny, quadratic orders, quaternion algebras, supersingular curves.
8. **Elliptic curves over $\mathbb{C}$**
   elliptic functions, Eisenstein series, the Weierstrass $\wp$-function,
   complex tori, the j-function, the uniformization theorem, isogenies.
9. **Modular curves**
   congruence subgroups, Riemann surfaces, modular functions.
10. **The theory of complex multiplication**
    ring class fields, Hilbert class polynomials, the CM method.
11. **Isogeny graphs**
    isogeny volcanoes, supersingular isogeny graphs, isogeny-based cryptography.
12. **Divisors and pairings**
    divisor class groups, pairings, Miller's algorithm, pairing-based cryptography.
13. **Elliptic curves over $\mathbb{Q}$**
    Mordell's theorem, 2-descent, Weil-Châtelet, Selmer, and Shafarevich–Tate groups.
14. **L-functions**
    Modular forms, modularity, the Birch and Swinnerton-Dyer conjecture.