Mathematics 574 Topics in Number Theory Fall 2013

Projects for Math 574

Possible topics for a 5-10 page treatment of a topic in elliptic curves due on or before December 20, 2013 are listed below. If you wish to do a project in some other aspect of elliptic curves contact me.

1. Elliptic curves over the complex field
   Every compact Riemann surface is an algebraic variety, so for any lattice $\Lambda \subset \mathbf{C}$ the complex torus $\mathbf{C}/\Lambda$ is an algebraic variety. The Weierstrass function and its derivative provide explicit formulas for the functions appearing in the Riemann-Roch theorem.

2. Explicit Weil pairing examples
   Compute the Weil pairing on points of order 2 and 3 on the curve $y^2 = x^3 - x$ over a field with p elements for select p a prime congruent to 3 modulo 4.

3. Supersingular elliptic curves and endomorphisms
   When the dual isogeny to the Frobenius endomorphism is purely inseparable there are strong conditions on the isomorphism class of the curve. Study such supersingular curves, their endomorphism rings, etc.

4. Poncelet's Porism
   Let C, D be irreducible plane conics. Let P be a point on C. The line ℓ through P and tangent to D hits C at a point Q on C. Continue in this manner to produce a sequence of points on C. Poncelet's result is that cardinality of the number of points obtained is independent of the starting point P. The set of pairs (P, ℓ) is the intersection of two quadrics in P^3 so that the operations may be interpreted in terms of maps of an elliptic curve to itself.

5. Elliptic integrals
   Explain what the relation is between elliptic curves and ellipses. Describe the arithmetic-geometric mean algorithm for computation of the integral of a regular differential over the real points of an elliptic curve.

6. Division of the lemniscate
   Discuss Abel's proof that the lemniscate $(x^2 + y^2)^2 = x^2 - y^2$ can be divided into N equal length segments by straightedge and compass if and only if the circle can be divided into N equal arcs by straightedge and compass.

7. Cryptography and elliptic curves
   Any group can serve cryptographic purposes by introducing the discrete logarithm problem or other means. For an elliptic curve the Weil pairing reduces the discrete logarithm problem to one in the multiplicative group of a field.

8. Elliptic curves with complex multiplication

An elliptic curve over the rationals with endomorphism ring strictly larger than the integers has close relations to quadratic imaginary fields. Study the Tate module and L-series for such curves.