Exercise Set 5 – Arithmetic Geometry, Frank Thorne (thorne@math.sc.edu)

Due Friday, March 5, 2016

(1) Consider the elliptic curve $E \ : \ Y^2 = X^3 - 3$.

Prove that E defines an elliptic curve over $\mathbb{F}_p$ for all primes $p \leq 20$ with one exception. For every prime p for which E defines an elliptic curve over $\mathbb{F}_p$, compute $\#E(\mathbb{F}_p)$, whether by hand or by computer. Check that your results are consistent with Hasse's theorem.

(2) (a) Prove that there are $\frac{q^{n+1}-1}{q-1} = 1 + q + q^2 + \cdots + q^n$ points in $\mathbb{P}^n(\mathbb{F}_q)$.

(b) Prove that the Hasse-Weil zeta function of $\mathbb{P}^n$ over $\mathbb{F}_p$ is

$$Z(\mathbb{P}^n/\mathbb{F}_p; T) = \frac{1}{(1-T)(1-pT)(1-p^2T)\cdots(1-p^nT)}.$$

(3) Again consider the elliptic curve $E \ : \ Y^2 = X^3 - 3$, this time only in characteristic 2.

(a) Explicitly construct the finite fields $\mathbb{F}_2$, $\mathbb{F}_4$, and $\mathbb{F}_8$, and count the number of points (including the point at infinity!) that E has over each of these fields.

(b) Recall that, by the Weil conjectures, we have

$$Z(E/\mathbb{F}_2; T) = \frac{1 + aT + 2T^2}{(1-T)(1-2T)}.$$

Prove that $a = \#E(\mathbb{F}_2) - 3$, and thereby write down the exact form of the zeta function.

(c) Prove an explicit formula for $\#E(F_{2^r})$, valid for all positive integers r, and verify that it matches your counts for $\mathbb{F}_4$ and $\mathbb{F}_8$.