Exercise Set 4 – Arithmetic Geometry, Frank Thorne (thorne@math.sc.edu)

Due Friday, March 6, 2016

(1) Consider the variety V described by the vanishing of $y^3 = (x-1)(x-2)(x-3)(x-4)(x-5)$ in $\mathbb{A}^2(\mathbb{F}_p)$.

  (a) Compute $\#V(\mathbb{F}_p)$ for all primes $p < 10$.

  (b) Guess a pattern or an approximate pattern. What do you think that $\lim_{p\to\infty} \frac{\#V(\mathbb{F}_p)}{p}$ is?

(2) Consider the variety V described by the vanishing of $X^3 + Y^3 + Z^3$ in $\mathbb{P}^2(\mathbb{F}_p)$. Then this is an elliptic curve (when it is smooth, and provided that a group identity is chosen), although not in Weierstrass form.

Gauss proved an amazing formula for $\#V(\mathbb{F}_p)$. If $p \not\equiv 1 \pmod 3$, then $\#V(\mathbb{F}_p) = p + 1$. If $p \equiv 1 \pmod 3$, then there are integers A and B with

$$4p = A^2 + 27B^2,$$

which are unique up to changing their signs.[1] Choosing the sign of A such that $A \equiv 1 \pmod 3$, we have

$$\#V(\mathbb{F}_p) = p + 1 + A.$$

  (a) Prove the $p \equiv 1 \pmod 3$ case. (This is easy: the condition on p guarantees that the map $t \mapsto t^3$ is a bijection on $\mathbb{F}_p$.)

  (b) Verify Gauss's result in the case that $p = 13$.

  (c) What upper bound on $|\#V(\mathbb{F}_p) - (p + 1)|$, as a function of p, is immediate from Gauss's theorem?

[1] No, this isn't obvious.