

Problem Set 3 – Arithmetic Geometry, Frank Thorne (thorne@math.sc.edu)

Due Friday, February 12, 2016

Choose one. (Not that I discourage you from solving both.)

(1) (Do not use the Riemann-Roch theorem for any of this. Please argue directly.)

- (a) Prove that the degree 0 part of the Picard group of \mathbb{P}^1 is trivial.
- (b) Let L be a line in \mathbb{P}^2 . Prove that the degree 0 part of the Picard group of L is trivial.
- (c) Let $V = V(X^2 + Y^2 - Z^2)$ in \mathbb{P}^2 . Prove that the degree 0 part of the Picard group of V is trivial.
- (d) Let E be an elliptic curve. Prove that the degree 0 part of the Picard group of V is *not* trivial.

You might follow (but in your own words please) the elegant proof here: <http://www.mathematik.uni-kl.de/~gathmann/class/alggeom-2014/chapter-14.pdf>

(2) (Suitable if you enjoy computer programming.)

Using Python, Java, Sage, PARI/GP, etc. (or any other language of your choice), write a computer program which accepts the following input:

- The equation of an elliptic curve E (which you may assume is of the form $y^2 = x^3 + Ax + B$).
- Two points P_1 and P_2 on E , each given as ordered pairs (x_i, y_i) . You may assume that neither is the point at infinity, but do not assume they are unequal.

Your program should return the coordinates of $P_1 + P_2$.

Please use rational number rather than floating point arithmetic if this is natively supported by your programming language of choice. But *please do the arithmetic from scratch!* (i.e., don't use PARI/GP and Sage's built in functionality to do exactly this. Of course, this is a great way to check your work.)