Problem Set 7 – Arithmetic Geometry, Frank Thorne (thorne@math.sc.edu)

Due Tuesday, May 5, 2020

(1) Suppose that a is an integer not divisible by p. Then prove that $\frac{1}{a} \in \mathbb{Z}_p$. Writing

$$\frac{1}{a} = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots ,$$

with each b_i satisfying $0 \leq b_i \leq p - 1$, prove that the sequence of b_i is periodic, and determine its period.

(2) For which integers n does the equation $x^2 - n = 0$ have a solution $x \in \mathbb{Z}_2$? (Prove your claims.)

(3) In computing the rank of the elliptic curve $y^2 = x^3 + 17x$, one is led by the method in Silverman-Tate to determine whether or not the equation

$$N^2 = 17M^4 - 4e^4$$

has a nontrivial integer solution.

As it turns out, it doesn't. However, it has solutions in $\mathbb{Z}_p$ for every prime p, making it a counterexample to the Hasse Principle. Prove that that there are solutions in $\mathbb{Z}_p$.

HInts. Don't go looking for 'unique' or 'special' solutions; there will be lots, and just cook them up using whatever *ad hoc* method you can come up with. You will probably want to make aggressive use of Hensel's Lemma; see e.g. Keith Conrad's notes here:

`https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf`