NUMBER THEORY SEMINAR
ASSIGNMENT 6
DUE DATE: DECEMBER 19, 2018

Exercise 1. *Let p be a prime, and $q = p^m$ a prime power. Show that the binomial coefficients $\binom{q}{j}$ are divisible by p for $1 \leq j \leq q-1$.*

Let $\mathbb{F}_q$ be a finite field with q elements, with q odd. Let $Q(T) \in \mathbb{F}_q[T]$ be a polynomial of positive degree. For any extension field E of $\mathbb{F}_q$, let

$$C(E) = \{(x, y) \in E \times E : y^2 = Q(x)\}$$

(C is called a "hyper-elliptic curve over $\mathbb{F}_q$" when $\deg Q > 2$).

Exercise 2. *a) For a quadratic polynomial $Q(T) = T^2 + a \in \mathbb{F}_q[T]$, show that if $a \neq 0$ then*

$$\#C(\mathbb{F}_q) = q - 1.$$

b) What happens when $a = 0$?

Exercise 3. *Show that*

$$\#C(\mathbb{F}_q) = q + \sum_{\alpha \in \mathbb{F}_q} Q(\alpha)^{(q-1)/2}.$$

Exercise 4. *Assume now that $Q \in \mathbb{F}_q[T]$ is monic irreducible. Show that*

$$\#C(\mathbb{F}_q) = q + (-1)^{\frac{q-1}{2} \deg Q} \sum_{\alpha \in \mathbb{F}_q} \left(\frac{x - \alpha}{Q} \right)_2$$