MATH-GA 2420.006 : Homework 2; due by Thursday February 18 morning (before 10am), late submission implies -50% of this homework grade; send the solutions to pirutka@cims.nyu.edu

1. Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Show that the group $E(\mathbb{F}_q)$ is either a cyclic group $\mathbb{Z}/n$ for some $n \geq 1$, or the group $\mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2$ with $n \geq 1$ and $n_1, n_2 \geq 1$ integers, $n_1 \,|\, n_2$.

2. Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p. Assume $E(\mathbb{F}_q) = \mathbb{Z}/n \oplus \mathbb{Z}/n$.

   (a) Show that $(n, p) = 1$.

   (b) Show that $E(\overline{\mathbb{F}}_q)[n] \subset E(\mathbb{F}_q)$. Deduce that $\mu_n \subset \mathbb{F}_q$.

   (c) Let $a = q + 1 - \#E(\mathbb{F}_q)$. Deduce that $a \equiv 2 (\text{mod}\, n)$.

   (d) Show that $q = n^2 + 1$ or $q = n^2 \pm n \pm 1$ or $q = (n \pm 1)^2$.

3. (a) Let α be an endomorphism of E and $(n, char.k) = 1$.

      i. Show that α induces an endomorphism α_n of $E[n]$.

      ii. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ the matrix of α_n in the base $\{T_1, T_2\}$. Show that

      $$deg\, \alpha \equiv det(\alpha_n) (\text{mod } n)$$

      (one could express $\zeta^{deg\, \alpha}$ in terms of a, b, c, d.)

   (b) Let α, β be two endomorphisms of E and r, s two integers.

      i. Show that

      $$det(r\alpha_n + s\beta_n) - r^2 det\alpha_n - s^2 det\beta_n = rs(det(\alpha_n + \beta_n) - det\alpha_n - det\beta_n)$$

      (one can start by showing that $det(\alpha_n + \beta_n) - det\alpha_n - det\beta_n = Trace(\alpha_n \beta_n^*)$, where β_n^* is the adjoint matrix : if $\beta_n = \left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right)$, then $\beta_n^* = \left(\begin{smallmatrix} t & -y \\ -z & x \end{smallmatrix}\right)$).

      ii. Deduce that

      $$deg\, r\alpha + s\beta = r^2 deg\, \alpha + s^2 deg\, \beta + rs(deg\, (\alpha + \beta) - deg\, \alpha - deg\, \beta).$$

4. (a) Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, $q = p^r$, and let $a_q = q + 1 - \#E(\mathbb{F}_q)$. As before, we denote ϕ_q the Frobenius morphism on E and for any integer m prime to q one denote $(\phi_q)_m$ the endomorphism induced by ϕ_q on $E(\overline{\mathbb{F}}_q)[m]$. Show that

   $$det(\phi_q)_m \equiv q \,(\text{mod } m) \text{ and } Trace(\phi_q)_m \equiv a_q \,(\text{mod } m)$$

   (One could use that $\#Ker(\phi_q - 1) = deg\,(\phi_q - 1) = q + 1 - a_q$, see the proof of Hasse theorem. Also use the formulas for det and Trace from the previous exercise)

(b) Deduce that the endomorphism $\phi_q^2 - a_q\phi_q + q$ is identically zero on $E(\overline{\mathbb{F}}_q)[m]$.

(c) Show that the kernel of the map $\phi_q^2 - a_q\phi_q + q$ is infinite; deduce that the polynomial $g(x) = x^2 - a_q x + q$ annihilates ϕ_q.

(d) Assume that b is an integer such that the polynomial $x^2 - bx + q$ annihilates ϕ_q. Deduce that $(a_q - b)$ annihilates $E(\overline{\mathbb{F}}_q)$ and finally that $a_q = b$.

(e) Let α, β be the roots of the polynomial $g(x)$ and let $g_n(x)$ be the polynomial

$$g_n(x) = x^{2n} - (\alpha^n + \beta^n)x^n + q^n.$$

Show that $g(x)$ divides $g_n(x)$ for all n. Deduce that

$$(\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = 0.$$

(f) Deduce that $E(\mathbb{F}_{q^n})$ has cardinality $q^n + 1 - (\alpha^n + \beta^n)$.

(g) We define the sets function of the curve E by

$$Z(E/\mathbb{F}_q, T) = exp(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n})\frac{T^n}{n}).$$

Show that $Z(E/\mathbb{F}_q, T)$ is a rational function

$$\frac{1 - a_q T + qT^2}{(1-T)(1-qT)}.$$

Additional exercise (DO NOT SUBMIT WITH THE HOMEWORK):

Let E be an elliptic curve $y^2 = x^3 + ax + b$ defined over a field k, $char(k) \neq 2, 3$. One defines the *division polynomials* $\psi_m(x, y)$ in a recursive way : $\psi_0 = 0$, $\phi_1 = 1$,
$\psi_2 = 2y$
$\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$
$\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$
$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$, $m \geq 2$
$\psi_{2m} = [\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)]/2y$, $m \geq 3$.

1. Show that ψ_n is a polynomial in x, y^2 if n is odd and that $y\psi_n$ is polynomial in x, y^2, if n is even.

2. One defines $\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$
$\omega_m = [\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2]/4y$. Show that ϕ_n is a polynomial in x, y^2, that ω_n is a polynomial in x, y^2 if n is odd, and that $y\omega_n$ is a polynomial in x, y^2 if n is even.

3. By the previous question, on can define the polynomials $\phi_n(x)$ and $\psi_n^2(x)$ by replacing y^2 by $x^3 + ax + b$ in the polynomials $\phi_n(x, y)$ and $\psi_n^2(x, y)$. Show that $\phi_n(x)$ is the sum of x^{n^2} and the terms of lower degree, and that $\psi_n(x)^2$ is the sum of $n^2x^{n^2-1}$ and the terms of lower degree.

4. Show that for $P = (x, y)$ a point of E, one has

$$nP = \left(\frac{\phi_n(x)}{\psi_n(x)^2}, \frac{\omega_n(x, y)}{\psi_n(x)^3}\right)$$

5. Show that the polynomials $\phi_n(x)$ and $\psi_n(x)^2$ are relatively prime. Deduce the the multiplication by n map is of degree n^2.