1 Introduction

Let $\mathbb{F}_p$ be a finite field of characteristic $p \neq 2, 3$ and $\mathbb{F}_{p^n}$ be its extension of degree n. We wish to demonstrate the following theorem.

Theorem 1.1. *Let m be a prime which is not p and t an integer such that :*

1. $|t| < \sqrt{2p}$,
2. $X^2 - tX + q = (X - \alpha)(X - \beta) \bmod m$,
3. $(\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\} = \langle \alpha \rangle \times S$ *for S a subgroup of* $(\mathbb{Z}/m\mathbb{Z})^\times$,
4. $\mathrm{ord}_m(\alpha) = n$ *and* $\mathrm{ord}_m(\beta) \nmid n$.

Let $E/\mathbb{F}_p$ be an ordinary elliptic curve and t be the trace of its Frobenius map. In that situation, $\mathbb{F}_{p^n}$ is the smallest extension which contains points P of order m and for all such P in the eigenspace of α, the elliptic periods $\eta_\alpha(P)$ form a normal basis on $\mathbb{F}_p$.

More specifically, we wish to demonstrate the fact that said elliptic periods span $\mathbb{F}_{p^n}$. The proof is actually a secondary result from [1].

2 Characteristic zero

Let E be an elliptic curve and m be a prime. We recall that if m is an Elkies prime of E then the characteristic polynomial of the Frobenius map π, factors in two linear factor modulo m. Consequently, the reduction of π to $E[m]$ has two eigenspaces.

Let f_m be the division polynomial of order m and α one of the eigenvalue of $\pi \bmod m$, we note $f_{m,\alpha}$ the generator of one the eigenspaces; it is of degree $(m-1)/2$.

2.1 Preliminaries

We will use the notations of [1], let K be the field of definition of the Deuring lift

$$\widehat{E} : Y^2 = X^3 + \widehat{A}X + \widehat{B} \tag{1}$$

of the curve E. We introduce the two following extensions :

$$K_m = K[X]/(\widehat{f}_m(X)) \tag{2}$$

$$L_m = K_m[Y]/(Y^2 - (X^3 + \widehat{A}X + \widehat{B})) \tag{3}$$

of degree $m(m-1)/2$ for the former and 2 for the latter. We let $\Theta \in K_m$ be the residue class of X modulo $\widehat{f}_m$ and $\Gamma \in L_m$ be the residue class of Y in L_m.

Consider $P = (\Theta, \Gamma)$ the generic point of $\widehat{E}(L_m)$, for $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ the following action

$$\rho_a : \Theta \to ([a]\widehat{P})_X \tag{4}$$

defines an automorphism of K_m/K and

$$G = \{\rho_a : 1 \leq a \leq \frac{m-1}{2}\} \tag{5}$$

is a cyclic subgroup of $\mathrm{Gal}(K_m/K)$ and we let $K_0 = K_m^G$ be its fixed field. The polynomial $\widehat{f}_{m,\lambda}$ factor as

$$\widehat{f}_{m,\lambda}(T) = \prod_{a=1}^{\frac{m-1}{2}} (T - \rho_a(\Theta)) \tag{6}$$

in $K_0[T]$. Consequently, we have $K_m = K_0[X]/(\widehat{f}_{m,\lambda}(X))$. We can also define for all $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ the unique polynomial $\widehat{g}_a \in K_0[X]$ such that $\deg(\widehat{g}_a) < (m-1)/2$ and $\widehat{g}_a(\Theta) = \rho_a(\Theta)$, thanks to the fact that the extension is cyclic.

2.2 Elliptic Gaussian period

Since G is a cyclic group of order $(m-1)/2$, we can assume that

$$G \simeq (\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}. \tag{7}$$

Let $c \in (\mathbb{Z}/m\mathbb{Z})^\times$ be a generator. Let n be an odd divisor of $(m-1)/2$ and let $n' = (m-1)/(2n)$ be its cofactor such that $(n, n') = 1$. We write $h = c^n$ and $k = c^{n'}$, let $H = \langle h \rangle$ and $H' = \langle k \rangle$; consequently

$$(\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\} = H \times H' \tag{8}$$

For $0 \le i < n$, we define

$$\widehat{\eta}_i := \sum_{a \in H} \left([k^i a]\widehat{P} \right)_X = \sum_{a \in H} \rho_a(\rho_{k^i}(\Theta)) \tag{9}$$

We notice that $\widehat{\eta}_i = \rho_k^{(i)}(\widehat{\eta}_0)$ for all $0 \le i < n$; there is a cyclic action

$$\widehat{\eta}_0 \xrightarrow{\rho_k} \widehat{\eta}_1 \xrightarrow{\rho_k} \cdots \xrightarrow{\rho_k} \widehat{\eta}_{n-1} \xrightarrow{\rho_k} \widehat{\eta}_0 \tag{10}$$

from which we can deduce the following result.

Lemma 2.1. *The polynomial*

$$\widehat{M}(T) = \prod_{i=0}^{n-1} (T - \widehat{\eta}_i) \tag{11}$$

is irreducible with coefficients in $\mathcal{O}(K_0)$. It is the minimal polynomial of $\widehat{\eta}_0$ over K_0.

Proof. The $\widehat{\eta}_i$ are fixed by H, therefore we have $K_m^H = K(\widehat{\eta}_0)$ since the $\widehat{\eta}_i$ are polynomials of $\widehat{\eta}_0$ because of the cyclic nature of the action. In other word, we have the following situation

$$\begin{tikzcd}[arrows=dash]
 & K_m \arrow[dl, "H"'] \arrow[dd, "G"] \\
K(\eta_0) \arrow[dr, "G/H = H'"'] & \\
 & K_0
\end{tikzcd} \tag{12}$$

Moreover, the action of H' is permuting the $\widehat{\eta}_i$, then every symetrical polynomials of the $\widehat{\eta}_i$ are fixed by H', so the coeffectients $\widehat{M}(T)$ are in K_0. From there we can deduce than any combination of less than n factor of $\widehat{M}(T)$ would not be in $K_0[T]$, so the polynomial is indeed irreducible. $\square$

3 Finite field case

In respect with the notations of [1], we let

$$\mathcal{A}_0 = \mathbb{F}_p[X]/(f_{m,\lambda}(X)) \tag{13}$$

and

$$\mathcal{A} = \mathbb{F}_p[X]/(Y^2 - (X^3 + AX + B), f_{m,\lambda}(X)). \tag{14}$$

Let θ and γ be the residue class of X and Y in $\mathcal{A}$. We write $P = (\theta, \gamma)$ the generic point in the eigenspace of α. Like in section 2.1, for $a(\mathbb{Z}/m\mathbb{Z})^\times$ we define the unique polynomials g_a of degree inferior to $(m-1)/2$ such that $g_a(\theta) = ([a]P)_X \in \mathcal{A}$.

Fact 3.1. *If m is an Elkies prime for $E/\mathbb{F}_p$, then there exists a prime $\mathfrak{p}$ of $\mathcal{O}(K_0)$ above p such that $\widehat{f}_{m,\lambda} = f_{m,\lambda} \bmod \mathfrak{p}$, i.e. the polynomial $\widehat{f}_{m,\lambda}$ is a cyclic lift of $f_{m,\lambda}$; in a similar way, the $\widehat{g_a}$ are cyclic lifts of g_a for all $a \in (\mathbb{Z}/m\mathbb{Z})^\times$.*

Proof. TODO $\square$

Then by the definition of g_a, we can write

$$f_{m,\lambda}(Z) = \prod_{a=1}^{\frac{l-1}{2}} (Z - g_a(\theta)). \tag{15}$$

For $0 \leq i < q$, we define

$$\eta_i = \sum_{a \in H} g_a(g_{k^i}(\theta)) \tag{16}$$

in particular $\eta_i = \widehat{\eta}_i \bmod \mathfrak{p}$. We remind that for odd $m \geq 3$, the discriminant of $f_m(X)$ satisfies the following relation

$$\mathrm{Disc}(f_m) = (-1)^{(m-1)/2} m^{(m^2-3)/2} (-\Delta)^{(m^2-1)(m^2-3)/24} \tag{17}$$

where $\Delta = \Delta(E)$ is the discriminant of E. Therefore the roots of $f_m(X)$, and $f_{m,\lambda}(X)$, are distinct. Which, in turn, implies that for $i \neq j$, we have $\eta_i \neq \eta_j$, because otherwise we could find a linear relation between the roots of $f_{m,\lambda}$. From there, we can conclude that the reduction of $\widehat{M}(T)$ is separated.

Finally, if we write $M(T) \in \mathbb{F}_p[T]$ the minimal polynomial of $\eta_0 \in \mathcal{A}_0$ and note that $M(T) = \widehat{M}(T) \bmod \mathfrak{p}$, we get that the degree of $M(T)$ is n.

4 Result

Now that we have everything we need, we can finish the proof of the theorem. Let $E/\mathbb{F}_p$ be an elliptic curve and m an Elkies prime for E. We also write α and β the two eigenvalues of the Frobenius of E.

We recall the hypothesis. One of the eigenvalue, say α, must be of order n in $(\mathbb{Z}/m\mathbb{Z})^\times$ and β must be of order not dividing by n. This means that n is an odd divisor of $\varphi(m) = m - 1$ and is prime to $(m-1)/n$; it is also prime to $(m-1)/2n$.

Let P by a point in the eigenspace of α. We then pick a generator $c \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that $\alpha = c^{n'}$ where $n' = (m-1)/2n$, so we can have the following situation

$$(\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\} = \langle \alpha \rangle \times H \tag{18}$$

where $H = \langle h \rangle$ and $h = c^n$.

From the previous section, we can deduce that the minimal polynomial of

$$\eta_\alpha(P) := \eta_0 = \sum_{a \in H} g_a(\theta) = \sum_{a \in H} ([a]P)_X \tag{19}$$

is $M(T)$ which is of degree n. As this stand for any point P of the eigenspace of α, we have therefore proved the point we wanted to.

References

[1] *Computing the Eigenvalue in the Schoof-Elkies-Atkin Algorithm using Abelian Lifts*, P. Mihăilescu, F. Morain & É. Schost, 2007, url : `http://hal.inria.fr/LIX/inria-00130142/en/`