Elliptic curves, number theory and cryptography –
Elliptiske kurver, talteori og kryptographi

2. handin – Endomorphisms, and elliptic curves in characteristic 2

Aurore Guillevic and Diego F. Aranha

Aarhus University
March 3, 2022

Due date: March 18, 4pm GMT+1 (16:00 Aarhus time)

1. Elliptic Curve With Endomorphism

Let \( p \) be a prime, \( p \geq 5 \), and let \( \mathbb{F}_p \) be the finite field with \( p \) elements.

Let \( E_2: y^2 = x^3 + a_2 x^2 + (a_2^2/8)x \) for some parameter \( a_2 \neq 0 \), defined over a finite field \( \mathbb{F}_p \) where \( p \geq 5 \) and \( -2 \) is a square modulo \( p \). The curve is ordinary.

Question 1. What is the \( j \)-invariant of the curve \( E_2 \)?

Hint: the \( j \)-invariant of a curve in Weierstrass form \( y^2 = x^3 + a_2 x^2 + a_4 x \) is 
\[ j(a_2, a_4) = \frac{256 (3a_4-a_2^2)^3}{a_1(4a_4-a_2^2)}. \]
Or, you can directly use SageMath, starting with:

\[
\begin{align*}
\text{QQa}.<a2> &= \text{QQ[]} \quad \# \text{a polynomial ring in one variable } a2 \\
E &= \text{EllipticCurve(QQa, [0,a2,0,a2^2/8])} \quad \# \text{a curve with coefficients } a1=0,a2,a3=0,a4=a2^2/8,a6=0
\end{align*}
\]

How asking SageMath about the \( j \)-invariant of \( E \)?

Question 2. Define the homomorphism

\[
\psi_2: (x, y) \rightarrow \begin{cases} 
0 & \text{if } (x, y) = (0, 0), \\
\left(-\frac{1}{2} \left(x + a_2 + \frac{a_2^2}{8}\right), \frac{y}{\sqrt{-2} \left(1 - \frac{a_2^2}{8}\right)} \right) & \text{otherwise.}
\end{cases}
\]

Check that \( \psi_2 \) is an endomorphism on \( E_2 \), that is given \( P(x, y) \in E \), \( \psi_2(x, y) \in E \).

Hint: SageMath can help you, start with

\[
\begin{align*}
\text{QQX}.<X> &= \text{QQ[]} \\
\text{QQ2}.<s2> &= \text{QQ.extension(X**2+2)} \\
\text{QQa2}.<a2> &= \text{QQ2[]} \quad \# \text{parameter } a2 \\
\text{QQa2xy}.<x,y> &= \text{QQa2[]} \quad \# \text{bivariate polynomial ring in } x, y \\
\text{F(X,Y) = 0} &= \text{with the parameter } a2 \\
\text{hint: use the method .numerator()} \text{ to get the numerator of a fraction}
\end{align*}
\]

Hint for pen-and-paper: use the curve equation to simplify the equations: \( \psi_{2,x} = -\frac{1}{2\sqrt{-2}} \left(x^3 + a_2 x^2 + \frac{a_2^2}{8}\right) = \frac{-y^2}{2\sqrt{-2}}. \)

What is the degree of \( \psi_2 \)? How many points are in the kernel of \( \psi_2 \)? What are the points in the kernel of \( \psi_2 \)?

Hint: you don’t need to show that \( \psi_2 \) is separable.

Question 3. One can check that \( \psi_2^2 \) corresponds to the multiplication by \(-2\) map \([-2]\) on \( E \). You are NOT expected to check that: this is assumed. What can you deduce about the characteristic polynomial of \( \psi_2 \) on \( E \)? What is the trace of \( \psi_2 \)?
Question 4. This curve $E_2$ has complex multiplication by $\sqrt{-2}$. Let $t$ be the trace of the Frobenius endomorphism on $E$, so that the curve order is $\#E(\mathbb{F}_p) = p + 1 - t$. One has $t^2 - 4p = -2g^2$ for some integer $g$.

Assume that the curve order has a large prime factor $r$ such that $r \mid \#E(\mathbb{F}_p)$, but $r^2$ does not divide $\#E(\mathbb{F}_p)$. What is the expression of the eigenvalue of $\psi_2$ (in terms of the trace $t$ and the parameter $g$), so that for a point $P$ of order $r$ ($P$ is a $r$-torsion point, and $E(\mathbb{F}_p)[r]$ is a cyclic subgroup), $\psi(P) = [\lambda \mod r]P'$? (two values for $\lambda$ are possible, give one such value).

Hint: you will need to compute $\sqrt{-2} \mod r$. remember that $\#E(\mathbb{F}_p) = p + 1 - t$ and let $y$ be such that $t^2 - 4p = -Dy^2$ for a square-free positive integer $D$. Then $p = (t^2 + Dy^2)/4$, and $\#E(\mathbb{F}_p) = (t^2 + Dy^2)/4 + 1 - t = (t^2 - 4 - 4t + Dy^2) = (t - 2)^2 + Dy^2)/4$. Let $r \mid \#E(\mathbb{F}_p)$ and $r$ coprime to 4, then $(t - 2)^2 + Dy^2 = 0 \mod r$. One can deduce $\sqrt{-D} \mod r$ in terms of $t$ and $y$.

Question 5. Compute a short basis for easy scalar decomposition according to Smith’s technique (Lecture of Tuesday, March 1).

2. SageMath part: the Bandersnatch curve

The Bandersnatch curve was introduced in 2021 in cryptography, and has Complex Multiplication by $\sqrt{-2}$. It has the following properties. There is a seed $u = -2^{63} - 2^{62} - 2^{60} - 2^{57} - 2^{48} - 2^{16}$, and $p = u^4 - u^2 + 1$ is a 255-bit prime. The Bandersnatch curve with $a_2 = 20$ has a large prime factor of 253 bits, and its quadratic twist with $a_2' = 4$ has a large prime factor of 244 bits.

Question 6. Consider the file `handin2.sage`. Compute the eigenvalue $\lambda_2 \mod r_2$ of $\psi_2$ on the curve $E_2$.

Compute the eigenvalue $\lambda_2' \mod r_2'$ of $\psi_2$ on the quadratic twist $E_2'$ (the subgroup order is not the same!).

Question 7. Compute (in SageMath) a short basis for easy scalar decomposition according to Smith’s technique (Lecture of Tuesday, March 1).

Check your result of Question 5.

3. Elliptic Curves in Characteristic 2

Question 8. Let $E(K) : y^2 + xy = x^3 + ax^2 + b$ be a non-supersingular elliptic curve defined over a binary field $K$. For $P = (x_1, y_1)$, the point doubling formula for $[2]P = (x_3, y_3)$ is given by (with $\lambda = x_1 + y_1/x_1$):

\[
\begin{align*}
x_3 &= \lambda^2 + \lambda + a = x_1^2 + b/x_1^2 \\
y_3 &= x_1^2 + \lambda x_3 + x_3.
\end{align*}
\]

Write the curve equation and point doubling formula in López-Dahab projective coordinates ($X_1/Z_1, Y_1/Z_1^2$). Both the input and output are given in LD projective coordinates. Optimize your formula such that it can be computed with 3 multiplications, 5 squarings and a few multiplications by $\{a, b\}$ in $K$.

Question 9. Kobitz curves, also known as anomalous binary curves are defined by the curve equation $E_a : y^2 + xy = x^3 + ax^2 + 1$ over $\mathbb{F}_{2^m}$ for $a \in \{0, 1\}$. Let $\mu = (-1)^{1-a}$. The order of a Kobitz curve can be computed as $\#E_a(\mathbb{F}_{2^m}) = 2^m + 1 - V_m$, where $V_m$ is the term of the Lucas sequence [2] given by the recurrence $V_{k+1} = \mu V_k - 2V_{k-1}$ for $k \geq 1$, $V_0 = 2$, $V_1 = \mu$.

Kobitz curves were standardized by NIST for prime degrees $m = \{163, 233, 283, 409, 571\}$. Write a SAGE script to find the mysteriously missing Kobitz curves in the interval $m \in \{163, 571\}$ for prime $m$ in which the order can be written as $h \cdot r$, such that $h \in \{2, 4\}$ and $r$ is prime.
References
