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 $E_2\colon y^2 = x^3 + a_2x^2 + (a_2^2/8)x$ 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 $y^2 = x^3 + a_2x^2 + a_4x$ is $j(a_2, a_4) = 256\frac{(3a_4-a_2^2)^3}{a_4^2(4a_4-a_2^2)}$. Or, you can directly use SageMath, starting with:

```
QQa.<a2> = QQ[] # a polynomial ring in one variable a2
E = EllipticCurve(QQa, [0,a2,0,a2^2/8]) # a curve with coefficients a1=0,a2,a3=0,a4=a2^2/8,
```

How asking SageMath about the j-invariant of E?

Question 2. Define the homomorphism

$$\psi_2\colon (x,y) \mapsto \begin{cases} \mathcal{O} & \text{if } (x,y) = (0,0), \\ \left(\frac{-1}{2}\left(x + a_2 + \frac{a_2^2}{8x}\right), \frac{y}{2\sqrt{-2}}\left(1 - \frac{a_2^2}{8x^2}\right)\right) & \text{otherwise.} \end{cases}$$

Check that ψ_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

```
QQX.<X> = QQ[]
QQ2.<s2> = QQ.extension(X**2+2)
# now, s2 corresponds to the square root of (-2), and SageMath knows that s2^2 = -2.
QQa2.<a2> = QQ2[] # parameter a2
# check that psi2 is an endomorphism, that is psi2(x,y) is on the curve
QQa2xy.<x,y> = QQa2[] # bivariate polynomial ring in x, y
# now define psix and psiy such that psi2(x,y) = (psix, psiy)
# and check that psix, psiy satisfy the curve equation of the form
# F(X,Y) = 0 with the parameter a2
# hint: use the method .numerator() to get the numerator of a fraction
```

Hint for pen-and-paper: use the curve equation to simplify the equations: $\psi_{2,x} = \frac{-1}{2x^2}\left(x^3 + a_2x^2 + \frac{a_2^2x}{8}\right) = \frac{-y^2}{2x^2}$.

What is the degree of ψ_2? How many points are in the kernel of ψ_2? What are the points in the kernel of ψ_2?

Hint: you don't need to show that ψ_2 is separable.

Question 3. One can check that ψ_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 ψ_2 on E? What is the trace of ψ_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 $t^2 - 4p = -2y^2$ for some integer y.

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 ψ_2 (in terms of the trace t and the parameter y), 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), $\psi(P) = [\lambda \bmod r]P$? (two values for λ are possible, give one such value).

Hint: you will need to compute $\sqrt{-2} \bmod r$. 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 $\#E(\mathbb{F}_p) = \frac{t^2+Dy^2}{4} + 1 - t = \frac{t^2+4-4t+Dy^2}{4} = ((t-2)^2 + Dy^2)/4$. Let $r \mid \#E(\mathbb{F}_p)$ and r coprime to 4, then $(t-2)^2 + Dy^2 = 0 \bmod r$. One can deduce $\sqrt{-D} \bmod r$ 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 $a_2^t = 4$ has a large prime factor of 244 bits.

Question 6. Consider the file `handin2.sage`. Compute the eigenvalue $\lambda_2 \bmod r_2$ of ψ_2 on the curve E_2.

Compute the eigenvalue $\lambda_2' \bmod r_2'$ of ψ_2 on the quadratic twist E_2^t (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 $\lambda = x_1 + y_1/x_1$):

$$x_3 = \lambda^2 + \lambda + a = x_1^2 + b/x_1^2$$
$$y_3 = x_1^2 + \lambda x_3 + x_3.$$

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. *Koblitz 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 Koblitz 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 $k \geq 1$, $V_0 = 2$, $V_1 = \mu$.

Koblitz curves were standardized by NIST for prime degrees $m = \{163, 233, 283, 409, 571\}$. Write a SAGE script to find the mysteriously missing Koblitz 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

[1] Simon Masson, Antonio Sanso, and Zhenfei Zhang. Bandersnatch: a fast elliptic curve built over the bls12-381 scalar field. Cryptology ePrint Archive, Report 2021/1152, 2021. `https://ia.cr/2021/1152`.

[2] Jerome A. Solinas. Efficient arithmetic on koblitz curves. *Des. Codes Cryptogr.*, 19(2/3):195–249, 2000.