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?

Solution 1. With SageMath:

```
QQa2.<a2> = QQ[]
E = EllipticCurve([0, a2, 0, a2**2/8, 0])
E.j_invariant()
8000
```

With the formula $j(a_2, a_4) = 256\frac{(3a_4 - a_2^2)^3}{a_4^2(4a_4 - a_2^2)}$, one obtains

$$j(E) = 256\frac{(3a_2^2/8 - a_2^2)^3}{(a_2^2/8)^2(4a_2^2/8 - a_2^2)} = 256\frac{(-5a_2^2/8)^3}{a_2^4/8^2(-a_2^2/2)} = 256\frac{-5^3a_2^6/4}{-a_2^6} = 64{\cdot}5^3 = 8000\,.$$

Moving the curve to short Weierstrass form: the change of variables is $(x, y) \mapsto (x - a_2/3, y)$. Remember that $(x+u)^3 = x^3+3ux^2+3u^2x+u^3$, hence $(x+a_2/3)^3 = x^3 + a_2x^2 + a_2^2x + a_2^3/3^3$. the result is $y^2 = x'^3 - 5/24a_2^2x' + 7/216a_2^3$, and the j-invariant, with $a = -5/24a_2^2$ and $b = 7/216a_2^3$, is $1728(4a^3)/(4a^3 + 27b^2) = 8000$.

```
QQa2.<a2> = QQ[]
QQa2x.<x> = QQa2[]
f = x^3 + a2*x^2 + a2^2/8*x
f(x-a2/3)
x^3 - 5/24*a2^2*x + 7/216*a2^3
b, a = (f(x-a2/3)).list()[0:2]
1728 * (4*a^3)/(4*a^3 + 27*b^2)
8000
```

Feedback 1. It is very important to check the pen-and-paper computation with SageMath, and even better to directly use SageMath to do the computation.

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 $P(x, y) \in E$, $\psi_2(x, y) \in E$. 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?

Solution 2. With SageMath.

```
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
psix = -(x + a2 + a2**2/(8*x))/2
psiy = y*(1-a2**2/(8*x**2))/(2*s2)
x3 = psix
y3 = psiy

f = x**3 + a2*x**2 + a2**2/8*x # right-hand side of E
F = x**3 + a2*x**2 + a2**2/8*x - y**2 # full equation of the curve E
F(x3,y3)
(F(x3,y3)).numerator() % (F) # (x3,y3) is on the curve.
assert (F(x3,y3)).numerator() % (F) == 0 # (x3,y3) is on the curve.
```

Alternative. Rewrite

$$\psi_{2,x} = \frac{-1}{2x^2}\left(x^3 + a_2x^2 + \frac{a_2^2x}{8}\right) = \frac{-y^2}{2x^2}$$

because the curve equation is $y^2 = x^3 + a_2x^2 + a_2^2/8x$. Then he right-hand side of the curve equation evaluated at $\psi_{2,x}$ is

$$\psi_{2,x}^3 + a_2\psi_{2,x}^2 + \frac{a_2^2}{8}\psi_{2,x} = \psi_{2,x}\cdot\left(\psi_{2,x}^2 + a_2\psi_{2,x} + \frac{a_2^2}{8}\right) = \frac{-y^2}{2x^2}\left(\psi_{2,x}^2 + a_2\psi_{2,x} + \frac{a_2^2}{8}\right)$$

Now we compute the term in the right-hand side parenthesis with

$$\psi_{2,x} = -\left(\frac{x}{2} + \frac{a_2}{2} + \frac{a_2^2}{16x}\right), \quad \psi_{2,x} + a_2 = -\left(\frac{x}{2} - \frac{a_2}{2} + \frac{a_2^2}{16x}\right),$$

$$\psi_{2,x}(\psi_{2,x} + a_2) = \left(\frac{x}{2} + \frac{a_2}{2} + \frac{a_2^2}{16x}\right)\left(\frac{x}{2} - \frac{a_2}{2} + \frac{a_2^2}{16x}\right) = \left(\frac{x}{2} + \frac{a_2^2}{16x}\right)^2 - \frac{a_2^2}{4}$$

$$\psi_{2,x}(\psi_{2,x} + a_2) + \frac{a_2^2}{8} = \left(\frac{x}{2} + \frac{a_2^2}{16x}\right)^2 - \frac{a_2^2}{8} = \left(\frac{x^2}{4} + \frac{a_2^4}{2^8x^2} + \frac{a_2^2}{16}\right) - \frac{a_2^2}{8}$$

$$\psi_{2,x}^2 + \psi_{2,x}a_2 + \frac{a_2^2}{8} = \frac{x^2}{4} + \frac{a_2^4}{2^8x^2} - \frac{a_2^2}{16} = \frac{x^2}{4}\left(1 - \frac{a_2^2}{4x^2} + \frac{a_2^4}{64x^4}\right) = \frac{x^2}{4}\left(1 - \frac{a_2^2}{8x^2}\right)^2$$

We obtain

$$\begin{aligned}\psi_{2,x}\cdot\left(\psi_{2,x}^2 + a_2\psi_{2,x} + \frac{a_2^2}{8}\right) &= \frac{-y^2}{2x^2}\left(\psi_{2,x}^2 + a_2\psi_{2,x} + \frac{a_2^2}{8}\right)\\ &= \frac{-y^2}{2x^2}\frac{x^2}{4}\left(1 - \frac{a_2^2}{8x^2}\right)^2\\ &= \frac{-y^2}{8}\left(1 - \frac{a_2^2}{8x^2}\right)^2\end{aligned}$$

and on the left-hand side evaluated at $\psi_{2,y}$, one obtains the same expression:

$$\psi_{2,y}^2 = \frac{-y^2}{8}\left(1 - \frac{a_2^2}{8x^2}\right)^2 .$$

We conclude that

$$\psi_{2,y}^2 = \psi_{2,x}^3 + a_2\psi_{2,x}^2 + \frac{a_2^2}{8}\psi_{2,x}$$

hence $(\psi_{2,x}, \psi_{2,y})$ is on the curve E.

The degree of ψ_2 is the degree of the rational function of $\psi_{2,x}$ in terms of x only, and $\psi_2(x) = (x^2 + a_2x + a_2^2/8)/x$, the degree of the numerator is 2 and the degree of the denominator is 1, therefore the degree of ψ_2 is 2.

The size of the kernel of ψ_2 is upper bounded by the degree of ψ_2, hence we know that $\#\ker\psi_2 \leq 2$. Actually we don't need to show that ψ_2 is separable: we know that $\mathcal{O} \in \ker\psi_2$, and moreover from the definition of ψ_2, $P(0,0) \in \ker\psi_2$, hence

$$\{\mathcal{O}, (0,0)\} \subseteq \ker\psi_2 \text{ and } \#\ker\psi_2 \leq 2 \implies \ker\psi_2 = \{\mathcal{O}, (0,0)\} \text{ and } \#\ker\psi_2 = 2 .$$

Feedback 2. Computing the kernel means solving for $P(x,y)$ in the equation $\psi_2(P) = \mathcal{O} = (\infty, \infty)$. Obtaining infinity corresponds to a division by zero, hence it corresponds to solving for the **denominators** to be zero, that is, solving for $x = 0$: one obtains the point $(0,0)$. Equivalently, in *projective coordinates* $P(X,Y,Z)$, the point at infinity is $\mathcal{O} = (0,1,0)$. The endomorphism in projective coordinates is

$$\psi_2 \colon (X,Y,Z) \mapsto \begin{cases} \mathcal{O} = (0:1:0) \text{ if } (X,Y) = (0,0), \\ \left(2X(8X^2 + 8a_2X + a_2^2), Y\sqrt{-2}(8X^2 - a_2^2), -32X^2\right) \text{ otherwise.} \end{cases}$$

Solving for $Z' = -32X^2 = 0$ gives the point $(0,0,1)$.

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?

Solution 3. The characteristic polynomial of ψ_2 is $X^2 + 2$. From the characteristic polynomial, we read that the coefficient of the X term is zero, and the trace of the endomorphism is 0.

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).

Solution 4. Here is a long version with comments. You can read about endomorphisms represented by 2×2 matrices in Washington's book page 80. Consider the r-torsion of E, we have $E[r] \simeq \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$. ψ_2 is an endomorphism, it can be represented by a 2×2 matrix

$$M = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

where a, b, c, d are coefficients modulo r that depend on the choice of the basis (P, Q) of $E[r]$. The matrix representation means

$$\psi_2(P) = aP + bQ$$
$$\psi_2(Q) = cP + dQ$$

and because it is assumed that $r \mid E(\mathbb{F}_p)$ but $r^2 \nmid E(\mathbb{F}_p)$, the point P can be taken in $E(\mathbb{F}_p)[r]$ but the point Q will not be defined over $\mathbb{F}_p$. With $P \in E(\mathbb{F}_p)$, because ψ_2 is $\mathbb{F}_p$-rational (remember that $\sqrt{-2} \in \mathbb{F}_p$), we know that $\psi_2(P) \in E(\mathbb{F}_p)[r]$, this implies $\psi_2(P) = aP + [0]Q$, in other terms, the point Q cannot be involved because it is defined over an extension. Therefore, $b = 0$, the matrix is

$$M = \begin{pmatrix} a & c \\ 0 & d \end{pmatrix}$$

and we are interested in computing the scalar a modulo r. This scalar is the *eigenvalue* of ψ_2 over $\mathbb{F}_p$, such that $\psi_2(P) = [a]P$.

From the characteristic polynomial of ψ_2 which is $X^2 + 2$, we know that $\psi_2 \circ \psi_2(P) = [-2]P$, and from the matrix representation, $\psi_2 \circ \psi_2(P) = [a^2]P$. The eigenvalue of ψ_2 modulo r is such that $a^2 = -2$, it is also a root of the characteristic polynomial $X^2 + 2 = 0$. The two roots are $\pm\sqrt{-2} \bmod r$. We are left with the computation of $\sqrt{-2} \bmod r$.

Finally, observe that the curve order is

$$\#E(\mathbb{F}_p) = p + 1 - t = \frac{t^2 + 2y^2}{4} + 1 - t = \frac{1}{4}\left(t^2 - 4t + 4 + 2y^2\right) = \frac{1}{4}\left((t-2)^2 + 2y^2\right)$$

Because r divides $p + 1 - t$, if we assume that r is coprime to 4, we can simplify the expression, and get

$$(t-2)^2 + 2y^2 = 0 \bmod r$$

and now, with $y \neq 0$,

$$\iff \left(\frac{t-2}{y}\right)^2 = -2 \bmod r \implies \frac{t-2}{y} = \pm\sqrt{-2} \bmod r \ .$$

The endomorphism ψ_2 has eigenvalue $\pm(t-2)/y \bmod r$.

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

Solution 5. The Frobenius endomorphism π_p has characteristic polynomial $\chi(X) = X^2 - tX + p$, it means $\pi_p \circ \pi_p - [t] \circ \pi_p + [p] = 0$. The roots of $\chi(X)$ are $\lambda_p = (t + \sqrt{t^2 - 4p})/2$ and $\mu_p = -\lambda_p + t$. We have $t^2 - 4p = -2y^2$ for some integer y (this is very specific to curves of j-invariant 8000). Because ψ_2 has eigenvalue $\sqrt{-2}$, and $\sqrt{t^2 - 4p} = \sqrt{-2}y$, we can express the Frobenius π in terms of ψ_2:

$$\pi = \frac{t}{2} + \frac{y}{2}\psi_2 \leftrightarrow \frac{t + y\sqrt{-2}}{2} = \frac{t}{2} + \frac{y}{2}\sqrt{-2} \ .$$

(There is a correspondence $\psi_2 \leftrightarrow \sqrt{-2}$, and $\pi \leftrightarrow (t + y\sqrt{-2})/2$).

We apply Theorem 2 of Smith paper: $\pi = y/2\psi_2 + t/2$, and $b = t/2$, $c = y/2$. The vectors are

$$\vec{b_1} = (b-1, c) = \left(\frac{t-2}{2}, \frac{y}{2}\right) \quad \vec{b_2} = (c\underbrace{\deg \psi_2}_{=2} + (b-1)\underbrace{t_{\psi_2}}_{=0}, 1-b) = \left(y, \frac{2-t}{2}\right) \ .$$

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 λ_2 mod r_2 of ψ_2 on the curve E_2.

Compute the eigenvalue λ_2' mod r_2' of ψ_2 on the quadratic twist E_2^t (the subgroup order is not the same!).

Solution 6. See the file `handin2_solutions.sage`.

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.

Solution 7. See the file `handin2_solutions.sage`.

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.

Solution 8. See the file `handin2_solutions.sage`.

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.

Solution 9. See the file `handin2_solutions.sage`.

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.