Elliptic curves, number theory and cryptography

4. handin – Isogenies

Aurore Guillevic and Diego F. Aranha

Aarhus University

March 31, 2022

Due date: April 22, 4pm GMT+2 (16:00 Aarhus time)

These exercises are taken from Pr. Tanja Lange lecture at
`https://www.hyperelliptic.org/tanja/teaching/isogeny-school21/exercises.pdf`
The corresponding lecture materials are at
`https://www.hyperelliptic.org/tanja/teaching/isogeny-school21/`
and Lorenz Panny materials at
`https://yx7.cc/docs/misc/isog_bristol_notes.pdf`

Question 1. Let

$$E_1/\mathbb{F}_{17} \colon y^2 = x^3 + 1, \quad E_2/\mathbb{F}_{17} \colon y^2 = x^3 - 10,$$
$$E_3/\mathbb{F}_{17} \colon y^2 = x^3 + 2x + 5\ .$$

```
p = 17
Fp = GF(p)
E1 = EllipticCurve(Fp, [0, 1])
E2 = EllipticCurve(Fp, [0, -10])
E3 = EllipticCurve(Fp, [2, 5])
```

(a) Check that

$$f \colon (x, y) \mapsto \left(\frac{x^3+4}{x^2}, y\frac{x^3-8}{x^3}\right)$$

defines a map $E_1 \to E_2$.
Hint: You only need to check that $f(x, y) \in E_2$. SageMath can help you to check your result (everything is performed modulo 17), replacing y^2 by $x^3 + 1$ when appropriate:

```
def f(x0, y0):
    return ((x0^3+4)/x0^2, y0*(x0^3-8)/x0^3)

p = 17
Fp = GF(p)
Fp.<x, y> = Fp[]
X, Y = f(x, y)
(X^3 - 10).numerator().factor()
(X^3 - 10).denominator().factor()
(Y^2).numerator().factor()
(Y^2).denominator().factor()
# to substitute y^2 by x^3+1:
Yn = Y.numerator().coefficient({y:1})
Yd = Y.denominator().coefficient({y:0})
Y2 = Yn^2 * (x^3+1) / Yd^2 # this is Y^2 with y^2 replaced by (x^3+1)
# now check for equality
```

(b) Determine the kernel of f.

(c) What is the degree of f?

(d) Calculate the points in the preimage of $(3, 0)$ under f.
Hint: To check with SageMath on such a tiny example, you can do something like

```
for P in E1:
    if P[0] == 0:
```

```
            print("P{} is on the curve E1".format(P))
        else:
            (xi, yi) = f(P[0], P[1])
            if xi == 3 and yi == 0:
                print("f({}, {}) = {}, {}".format(P[0], P[1], xi, yi))
```

(e) Compute the number of points on $E_1(\mathbb{F}_{17})$, $E_2(\mathbb{F}_{17})$, $E_3(\mathbb{F}_{17})$.
Hint: You can for example do an array

x, y	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8
x^3+1	-1	-2	6	-5	5	8	-7	0	1	2	-8	-6	-3	7	-4	4	3
y^2	-4	-2	2	8	-1	-8	4	1	0	1	4	-8	-1	8	2	-2	-4

then look for the matches $y^2 = x^3 + 1$. There are the affine points (not at infinity). SageMath code:

```
def centered(a, p):
    a0 = a % p
    if (p-a0) < a0:
        a0 = a0 - p
    return a0

x_coord = []
y_coord = []
for a in range(-8, 9):
    xa = centered(a^3+1, p)
    ya = centered(a^2, p)
    x_coord.append(xa)
    y_coord.append(ya)

print(", ".join([str(i) for i in x_coord]))
print(", ".join([str(i) for i in y_coord]))
```

(f) Compute $j(E_1)$, $j(E_2)$, $j(E_3)$. In SageMath: `E1.j_invariant()`.

(g) Show that E_1 and E_2 are not isomorphic over $\mathbb{F}_{17}$ but that they are isomorphic over $\mathbb{F}_{17^2}$.
Hint: Remember the form of an isomorphism $(x, y) \mapsto (xu^2, yu^3)$ for some non-zero well-chosen u.
Hint: If you intend to double-check with SageMath the isomorphism, you will need to define a quadratic exention of $\mathbb{F}_{17}$.

(h) Check that

$$g\colon (x, y) \mapsto \left(\frac{x^2+x+3}{x+1}, y\frac{x^2+2x+15}{(x+1)^2}\right)$$

defines a map $E_1 \to E_3$.
Hint: You only need to check that $g(x, y) \in E_3$. SageMath can help you to check your result (everything is performed modulo 17), replacing y^2 by $x^3 + 1$ when appropriate:

```
def g(x0, y0):
    return ((x0^2+x0+3)/(x0+1), y0*(x0^2+2*x0+15)/(x0+1)^2)

p = 17
Fp = GF(p)
Fp.<x, y> = Fp[]
X, Y = g(x, y)
# to substitute y^2 by x^3+1 in Y^2:
Yn = Y.numerator().coefficient({y:1})
Yd = Y.denominator().coefficient({y:0})
Y2 = Yn^2 * (x^3+1) / Yd^2 # this is Y^2 with y^2 replaced by (x^3+1)
```

(i) Determine the kernel of g.

(j) What is the degree of g?

Question 2. Let ℓ be a prime. Show that there are $\ell + 1$ size-ℓ subgroups of $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.
Hint: The ℓ-torsion has a 2-dimensional basis $\langle P, Q\rangle$. A point S or order ℓ can be written $S = [a]P + [b]Q$.

- If $a = 0$, the subgroup is $\langle Q\rangle$.
- If $b = 0$, the subgroup is $\langle P\rangle$.

- What are the generators of the other distinct subgroups of order ℓ?

→ How many different subgroups are there?

Question 3. Let $p = 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1$ and let $E_0 \colon y^2 = x^3 + x$.

```
p = 419
Fp = GF(p)
E0 = EllipticCurve(Fp, [1, 0])
```

(a) Find a point P of order 105 $(= (p+1)/4)$ on E_0.
Hint: with SageMath, you might need a `while` loop.
Compute $R = 35P$, a point of order 3.

(b) Vélu's formulas have a Montgomery form as follows. Let ℓ be a prime, P a point of order ℓ so that $\langle P \rangle$ is a subgroup of order ℓ, and let x_i denotes the x-coordinate of the point $[i]P$ in the subgroup generated by P. Define

$$\tau_\ell = \prod_{i=1}^{\ell-1} x_i, \quad \sigma_\ell = \sum_{i=1}^{\ell-1} x_i - \frac{1}{x_i}, \quad f_\ell(x) = x \prod_{i=1}^{\ell-1} \frac{x x_i - 1}{x - x_i} .$$

The ℓ-isogeny with kernel $\langle P \rangle$ is given by

$$\begin{array}{rcl} \phi_\ell \colon E^M : By^2 = x^3 + Ax^2 + x & \to & E_\ell^M : B_\ell y^2 = x^3 + A_\ell x^2 + x \\ (x, y) & \mapsto & (f_\ell(x), c_0 y f_\ell'(x)) \end{array}$$

where $A_\ell = \tau_\ell(A - 3\sigma_\ell)$ and $c_0^2 = \tau_\ell$.
Compute τ_3, σ_3 and $f_3(x)$ for $\langle R \rangle$. Compute the curve coefficient A_ℓ of the curve isogenous to E_0 under the 3-isogeny induced by R. What is the j-invariant of this isogenous curve? Check that the A-coefficient of the isogenous curve (that is, A_3) matches the subscript in Figure 3 in the lecture notes of Pr. Tanja Lange at `https://www.hyperelliptic.org/tanja/teaching/isogeny-school21/csidh-sidh-week-3.pdf` (look for a blue edge from E_0).

(c) Compute the image $P' = \varphi_3(P)$ under the 3-isogeny and verify that the resulting point P' has order 35. Why does this happen?

(d) Compute $7P'$ and use it to compute the 5-isogeny, getting the curve parameter and the image $P'' = \varphi_5(P')$. Check that P' has order 7 and that the curve coefficient matches the same Figure 3.

(e) Finally do the same for the 7-isogeny coming from P''.

Question 4. Let p be a prime with $p = 3 \bmod 4$. Show that $E \colon y^2 = x^3 + x$ has $p + 1$ points.
Hint: Remember that in $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ there are $(p-1)/2$ squares and as many non-squares.
Hint: Remember that -1 is not a square modulo p if $p = 3 \bmod 4$.
Hint: It was a homework of a previous week.

Question 5 (**Optional**)**.** Let $p = 431$ and note that $p + 1 = 432 = 2^4 \cdot 3^3$. The curve $E_0 \colon y^2 = x^3 + x$ is a supersingular curve over $\mathbb{F}_p$ and has $p+1$ points. Consider the curve over $\mathbb{F}_{p^2}$ where it has $(p+1)^2$ points. Find a basis of the 2^4-torsion and a basis of the 3^3-torsion subgroups, *i.e.*, find points P and Q of order 2^4 such that $\langle P \rangle \cap \langle Q \rangle = \mathcal{O}$ and points R and S of order 3^3 such that $\langle R \rangle \cap \langle S \rangle = \mathcal{O}$.
Hint: You can check this as $[8]P \neq [8]Q$ and $[9]R \neq \pm[9]S$.
Hint: For the 3^3 torsion points, remember how the negative direction is defined for CSIDH to find the independent points.