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 $E_1 \to E_2$.

(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.

(e) Compute the number of points on $E_1(\mathbb{F}_{17})$, $E_2(\mathbb{F}_{17})$, $E_3(\mathbb{F}_{17})$.

(f) Compute $j(E_1)$, $j(E_2)$, $j(E_3)$.

(g) Show that E_1 and E_2 are not isomorphic over $\mathbb{F}_{17}$ but that they are isomorphic over $\mathbb{F}_{17^2}$.

(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 $E_1 \to E_3$.

(i) Determine the kernel of g.

(j) What is the degree of g?

Solution 1.

(a) We only need to check that $f(x,y) = (f_x(x), f_y(x)) \in E_2$, that is it satisfies the curve equation. The shortest SageMath code: define the **Function Field** of the curve E_1. https://en.wikipedia.org/wiki/Algebraic_function_field#Example

```
def f(x0, y0):
    return ((x0^3+4)/x0^2, y0*(x0^3-8)/x0^3)
p = 17
Fp = GF(p)
# Definition of the function field of E1
K0.<x>= FunctionField(Fp)             # to allow inversion of the variable x
K0Y.<Y> = K0[]                        # polynomial ring in Y
K.<y> = K0.extension(Y**2 - x**3 - 1) # E1 equation
```

```
(fx, fy) = f(x,y)
check_f = fy^2 == fx^3 - 10
print("Check that Y^2 == X^3-10, where (X, Y) = f(x,y), (x,y) in E1: {}".format(check_f))
```

See the SageMath code for more details and alternatives.

(b) The x-values such that the denominator of f_x or f_y vanishes are the x-coordinates of points in the kernel of f. We solve

$$\left\{\begin{array}{ll} x = 0 \bmod 17 & \text{(denominator vanishes)} \\ y^2 - (x^3+1) = 0 \bmod 17 & (E_1) \end{array}\right. \iff \left\{\begin{array}{l} x = 0 \\ y^2 = 1 \end{array}\right. \iff (x,y) \in \{(0,1),(0,-1)\}$$

and moreover there is $\mathcal{O}$. Finally $\ker f = \{\mathcal{O},(0,1),(0,-1)\}$. See the SageMath code for an alternative.

(c) The **degree** of a homomorphism $(x,y) \mapsto (\phi_x(x), y\phi_y(x))$ is the highest degree of the polynomials at the numerator and denominator of ϕ_x, provided that the fraction is reduced, that is the GCD of the numerator and denominator is 1. (Washington's book page 51 for endomorphisms, p. 387 for homomorphisms).

First, checking that the two rational functions f_x and f_y are reduced. $f_x = \frac{x^3+4}{x^2}$, and $\gcd(x^3+4, x^2) = 1$ in $\mathbb{F}_{17}[x]$. $f_y = y\frac{x^3-8}{x^3}$ and $\gcd(x^3-8, x^3) = 1$ in $\mathbb{F}_{17}[x]$.

$$\deg f = \max(\text{numerator}(f_x), \text{denominator}(f_x)) = \max(3,2) = 3\ .$$

It turns out that f is an isogeny of degree 3, also noted a 3-isogeny, and its kernel is a subgroup of order 3, made of points of 3-torsion (whose order divides 3).

(d) See the SageMath code for an alternative solution.

$$f(x,y) = (3,0) \iff x \neq 0 \text{ and } \left\{\begin{array}{lcl} (x^3+4)/x^2 & = & 3 \bmod 17 \\ y(x^3-8)/x^3 & = & 0 \bmod 17 \end{array}\right.$$

One can start solving $y(x^3-8) = 0 \bmod 17 \iff y = 0$ or $x^3 = 8 \bmod 17 \iff x = 2$. There is no other root: $\zeta_3 2 \notin \mathbb{F}_{17}$ because $17 \equiv 2 \bmod 3$, in the case $p = 2 \bmod 3$ there is no primitive cube root of unity modulo p. Now $(E_1)\colon y^2 = x^3+1$ gives the other coordinate for $y = 0$ and $x = 2$: $\{(-1,0),(2,\pm 3)\}$. We just check that $f_x(2) = 3$ and $f_x(-1) = 3$. Because the homomorphism f has kernel of order 3, the preimage of a point is made of three points. Finally,

$$f^{-1}(3,0) = \{(-1,0),(2,3),(2,-3)\}\ .$$

(e) There are different options for that, the quickest is

```
E1.order()
E2.order()
E3.order()
```

whose answer is $18 = p+1$ in the three cases.

(f) Quickest way is with Sagemath and

```
E1.j_invariant()
E2.j_invariant()
E3.j_invariant()
```

Alternatively, $j(E) = 1728(4a^3)/(4a^3+27b^2)$ for a curve in short Weierstrass form. answers $j(E_1) = 0$, $j(E_2) = 0$, and $j(E_3) = 8$. We observe that $j(E_1) = j(E_2)$, that is E_1 and E_2 are isomorphic over some extension of $\mathbb{F}_{17}$.

(g) An isomorphism of curves in short Weierstrass form has the form (Washington's book page 46)

$$\begin{array}{rcl} E\colon y^2 = x^3+ax+b & \to & E'\colon y^2 = x^3+au^4x+bu^6 \\ (x,y) & \mapsto & (xu^2, yu^3) \end{array}$$

We look for $u \in \overline{\mathbb{F}_{17}}$ such that $b_1u^6 = b_2 \iff u^6 = -10 \bmod 17$. Note that $3^3 = 27 = 10 \bmod 17$, that is $(-3)^3 = -10 = u^6$, then $u^2 = -3$. But -10 is not a square modulo 17 (check that $(-10)^{(p-1)/2} = (-10)^8 \bmod 17 = -1 \neq 1$), and $u \notin \mathbb{F}_{17}$. A quadratic extension is required, such as $F_{17^2} = F_{17}(\sqrt{-3})$, so that $u = \sqrt{-3} \in \mathbb{F}_{17^2}$, and $u^6 = (-3)^3 = -10 = b_2 \bmod 17$. We conclude that because the equation $u^6 = -10 \bmod 17$ has no solution modulo p, but has a solution $u = \sqrt{-3}$ in $\mathbb{F}_{17^2}$, the curves E_1 and E_2 are isomorphic over $\mathbb{F}_{17^2}$ but not over $\mathbb{F}_p$. The isomorphism is

$$(x,y) \mapsto (-3x, -3\sqrt{-3}y)\ .$$

See the SageMath code for an alternative.

(h) Same procedure as for (a).

```
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)
# Definition of the function field of E1
K0.<x>= FunctionField(Fp)              # to allow inversion of the variable x
K0Y.<Y> = K0[]                         # polynomial ring in Y
K.<y> = K0.extension(Y**2 - x**3 - 1) # E1 equation
(gx, gy) = g(x,y)
check_g = gy^2 == gx^3 +2*gx + 5
print("Check that Y^2 == X^3+2*X+5, where (X, Y) = g(x,y), (x,y) in E1: {}".format(check_g))
```

(i) Same procedure as for (b). The x-values such that the denominator of g_x or g_y vanishes are the x-coordinates of points in the kernel of g. We solve

$$\left\{\begin{array}{ll} x+1 = 0 \bmod 17 & \text{(denominator vanishes)} \\ y^2-(x^3+1) = 0 \bmod 17 & (E_1) \end{array}\right. \iff \left\{\begin{array}{l} x=-1 \\ y^2=0 \end{array}\right. \iff (x,y) \in \{(-1,0)\}$$

and moreover there is $\mathcal{O}$. Finally $\ker g = \{\mathcal{O}, (-1,0)\}$. See the SageMath code for an alternative.

(j) Same procedure as for (c). The **degree** of a homomorphism $\phi\colon (x,y) \mapsto (\phi_x(x), y\phi_y(x))$ is the highest degree of the polynomials at the numerator and denominator, provided that the fraction is reduced, that is the GCD of the numerator and denominator is 1. (Washington's book page 51 for endomorphisms, p. 387 for homomorphisms).

First, checking that the two rational functions g_x and g_y are reduced. $g_x = \frac{x^2+x+3}{(x+1)^2}$, and $\gcd(x^2+x+1, x+1) = 1$ in $\mathbb{F}_{17}[x]$. $g_y = y\frac{x^2+2x+15}{(x+1)^3}$ and $\gcd(x^2+2x+15, x+1) = 1$ in $\mathbb{F}_{17}[x]$.

$$\deg g = \max(\text{numerator}(g_x), \text{denominator}(g_x)) = \max(2,1) = 2\ .$$

It turns out that g is an isogeny of degree 2, also noted a 2-isogeny, and its kernel is a subgroup of order 2, made of points of 2-torsion (whose order divides 2).

Question 2. Let ℓ be a prime. Show that there are $\ell+1$ size-ℓ subgroups of $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.

Solution 2. Let's consider the possible subgroups and their generator. The ℓ-torsion has a structure of two-dimensional vector space with a basis $\{P, Q\}$ for two points P, Q of order ℓ generating two distinct subgroups $\langle P\rangle$, $\langle Q\rangle$. It means that any point of order ℓ can be written as $iP + jQ$ for $i, j \in \{0, \ldots, \ell-1\}$. If $(i,j) = (a \cdot i_0, a \cdot j_0)$ for some non-zero $a \in \mathbb{Z}/\ell\mathbb{Z}$, then the point $iP + jQ$ is in the same subgroup as the point $i_0P + j_0Q$. Counting the distinct subgroups boilds down to counting the distinct pairs (i,j) that are linearly independant of each others. One can fix $i = 1$, then $P + jQ$ is a generator of the subgroup made of all the points of the form $aP + ajQ$ for $0 \le a \le \ell-1$ (including $\mathcal{O}$). The parameter j takes values in $\{1, \ldots, \ell-1\}$. For example the two subgroups made of $\{\mathcal{O}, P+bQ, 2(P+bQ), \ldots, (\ell-1)(P+bQ)\}$ of ℓ points ($b \ne 0$) and $\{\mathcal{O}, P+cQ, 2(P+cQ), \ldots, (\ell-1)(P+cQ)\}$ of ℓ points ($c \ne 0$) are distinct subgroups of intersection $\{\mathcal{O}\}$ whenever $c \ne b \bmod \ell$. There are $\ell-1$ such distinct subgroups made of distinct points. For $j = 0$, the subgroup is $\langle P\rangle$, that makes ℓ choices. Finally $(i,j) = (0,1)$ for $\langle Q\rangle$ completes the set of $\ell+1$ distinct subgroups.

In total there are $\ell+1$ subgroups of order ℓ. We counted the point at infinity $\mathcal{O}$ $\ell+1$ times in total (one for each subgroup). Deducing the redundant counts of $\mathcal{O}$, that makes $\ell(\ell+1) - \ell = \ell^2$ distinct points.

Another solution proposed by a student: let's enumerate the distinct non-zero ratio values i/j: there are $\ell-1$ such distinct ratios, hence $\ell-1$ distinct subgroups. Then adding $\langle P\rangle$ ($b = 0$, ratio being infinity) and $\langle Q\rangle$ ($a = 0$, ratio being 0) that makes $\ell+1$ subgroups. In other terms, it is the same as computing the number of points on the projective line $\mathbb{P}(\mathbb{Z}/\ell\mathbb{Z})$: $\{(0:1), (1:1), (2:1), \ldots, (\ell-1:1), (1,0)\}$ of $\ell+1$ points.

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

(a) Find a point P of order 105 ($= (p+1)/4$) on E_0. 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

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

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_3 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''.

Solution 3. See the SageMath code.

(a) Make sure to check that P has exactly order 105 by checking that any proper divisor of 105 does not map P to $\mathcal{O}$: $105P = \mathcal{O}$ but $15P \neq \mathcal{O}$, $21P \neq \mathcal{O}$, and $35P \neq \mathcal{O}$. $R = 35P$ should be one of $(178, 52)$, $(178, 367)$.

(b) $\tau_3 = 259$, $\sigma_3 = 243$, $f_3(x) = (259x^3 + 63x^2 + x)/(x^2 + 63x + 259)$. $A_3 = 158$, $j_3 = 356$.

(c) Note that φ_3 commutes with multiplication by 35: $[35]\varphi_3(P) = \varphi_3([35]P) = \varphi_3(R) = \mathcal{O}$ because by definition of φ_3, $\ker \varphi_3 = \langle R \rangle$. But $5\varphi_3(P) = \varphi_3(5P) \neq 0$ and $7\varphi_3(P) = \varphi_3(7P) \neq 0$ because $5P, 7P \notin \ker \varphi_3$. Hence $\varphi_3(P)$ has order exactly 35.

(d) $\tau_5 = 48$, $\sigma_5 = 242$, $A_5 = 390$, $f_5 = (48x^5 + 369x^4 + 149x^3 + 368x^2 + x)/(x^4 + 368x^3 + 149x^2 + 369x + 48)$, $j_5 = 0$.

(e) $\tau_7 = 79$, $\sigma_7 = 305$, $A_7 = 6$, $f_7 = (79x^7 + 254x^6 + 311x^5 + 265x^4 + 303x^3 + 96x^2 + x)/(x^6 + 96x^5 + 303x^4 + 265x^3 + 311x^2 + 254x + 79)$, $j_7 = 62$.

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.

Solution 4. This exercise is taken from Wouter Castryck's lectures at the online isogeny summer school in 2021. Here is a solution.

Define the three sets

$$\begin{array}{rcl} S_1 & = & \big\{x \in \mathbb{F}_p | x^3 + x \text{ is a non-zero square}\big\} \\ S_2 & = & \big\{x \in \mathbb{F}_p | x^3 + x = 0\big\} \\ S_3 & = & \big\{x \in \mathbb{F}_p | x^3 + x \text{ is not a square}\big\} \end{array}$$

First note that the three sets define a partition of $\mathbb{F}_p$, and

$$\#S_1 + \#S_2 + \#S_3 = \#\mathbb{F}_p = p \ . \tag{1}$$

For each $x \in S_1$, there are two points $(x, \pm y)$ on E, where $y = \sqrt{x^3 + x}$. For each $x \in S_2$, there is one point $(x, 0)$ on E. For each $x \in S_3$, there is no corresponding point on E. Hence the order of E is $\#E(\mathbb{F}_p) = 2\#S_1 + \#S_2 + 1$, the $+1$ accounting for $\mathcal{O}$.

The sets S_1 and S_3 are in bijection with the map $x \mapsto -x$ because -1 is not a square in $\mathbb{F}_p$, for $p = 3 \bmod 4$. Indeed, $(-1)^{(p-1)/2} = -1$ because $(p-1)/2$ is odd. Thus $\#S_1 = \#S_3$. From (1), $2\#S_1 + \#S_2 = p$. Finally $\#E(\mathbb{F}_p) = 2\#S_1 + \#S_2 + 1 = p + 1$.