Elliptic curves, number theory and cryptography

1. hand-in – Montgomery form of elliptic curves

Aurore Guillevic and Diego F. Aranha

Aarhus University

February 10, 2022

Due date: February 25, 4pm GMT+1 (16:00 Aarhus time)

Let p be a prime with $p \neq 2, 3$ and let $\mathbb{F}_p$ be the finite field with p elements. Let $A \in \mathbb{F}_p$ and consider the equations:

$$E^M : y^2 = x^3 + Ax^2 + x \tag{1}$$

$$E^M : Y^2Z = X^3 + AX^2Z + XZ^2 \tag{2}$$

1. Group law

Question 1. Show that the equations define an elliptic curve E^M in $\mathbb{A}^2$ (eq. (1)) and $\mathbb{P}^2$ (eq. (2)) if and only if $A \neq \pm 2$. This is called an elliptic curve in Montgomery form.

Solution 1. For the affine equation of the curve, one option is to compute the discriminant (denominator of the j-invariant) and check when it is non-zero. In Montgomery coordinates, the j-invariant is

$$j(E^M) = 256\frac{(A^2-3)^3}{A^2-4}$$

and its denominator is non-zero when $A \neq \pm 2$.

Alternatively, one could check the condition so that $f(x) = x^3 + Ax^2 + x$ has no multiple root: $x_0 = 0$ is a root of $f(x)$, then $f(x) = x(x^2 + Ax + 1)$. The two other roots are $x_1 = (-A + \sqrt{A^2-4})/2$, $x_2 = (-A - \sqrt{A^2-4})/2$. They are both non-zero (because the constant coefficient of $x^2 + Ax + 1$ is non-zero), then distinct from x_0. We only need to ensure that $x_1 \neq x_2$, that is, $\sqrt{A^2-4} \neq 0$, equivalently, $A^2 \neq 4 \iff A \neq \pm 2$.

Long version, but it's better to use one of the shortcuts above. The curve is defined by a cubic equation, and $(0, 0)$ is a $\mathbb{F}_p$-rational point on the curve in affine coordinates, $(0 : 0 : 1)$ in projective coordinates. We only need to check that the curve has no singular point (in other words, that the curve is smooth).

In affine coordinates, a singular point of the curve is a solution to a system of two equations, where $f(x, y) = y^2 - x^3 - Ax^2 - x$,

$$\begin{cases} (x,y) \in E \\ \frac{\partial f}{\partial x} = -3x^2 - 2Ax - 1 = 0 \\ \frac{\partial f}{\partial y} = 2y = 0 \end{cases} \iff \begin{cases} y^2 = x(x^2 + Ax + 1) \\ -3x^2 - 2Ax - 1 = 0 \\ y = 0 \end{cases}$$

We immediately get $y = 0$, and see that $x = 0$ gives no solution, so we focus on $x^2 + Ax + 1 = 0$ for the first equation. It would not be very direct to start writing $x = \frac{2A \pm \sqrt{A^2-3}}{3}$ or $x = \frac{-A \pm \sqrt{A^2-4}}{2}$. Instead, we solve simultaneously the two equations in x: three times the first equation added to the second cancels the squares and we obtain $Ax + 2 = 0$. Inserting $Ax = -2$ in the first equation, we obtain $x^2 = 1$ hence $x = \pm 1$ then $A = \mp 2$. Finally, a singular point is $(\pm 1, 0)$ with

$A = \mp 2$. So when $A \neq \pm 2$, there is no singular point, the curve is smooth, and then E^M is an elliptic curve.

In projective coordinates, with $F(X, Y, Z) = Y^2 Z - X^3 - AX^2 Z - XZ^2$, the singular points satisfy

$$\begin{cases} \frac{\partial f}{\partial X} = -3X^2 - 2AZX - Z^2 = 0 \\ \frac{\partial f}{\partial Y} = 2YZ = 0 \\ \frac{\partial f}{\partial Z} = Y^2 - AX^2 - 2XZ = 0 \end{cases} \iff \begin{cases} X = 0 \\ Y = 0 \\ Z = 0 \end{cases} \text{or} \begin{cases} -3X^2 - 2AZX - Z^2 = 0 \\ Y = 0 \\ X(-AX - 2Z) = 0 \end{cases}$$

but $(0, 0, 0) \notin \mathbb{P}^2$ and we discard it, and the non-zero solution to the second system of equations is

$$\begin{cases} 3Z^2(1 - 4/A^2) = 0 \\ Y = 0 \\ A/2X + Z = 0 \end{cases} \iff \begin{cases} X = -2Z/A \\ Y = 0 \\ Z \neq 0, A = \pm 2 \end{cases}$$

A singular point is $(\mp\lambda, 0, \lambda)$ for any $\lambda \neq 0$ (the equivalence class is $(\mp 1 : 0 : 1)$), for $A = \pm 2$. In projective coordinates, $A \neq \pm 2$ is required to avoid having a singular point.

Question 2. Derive the formulas for addition and doubling of points on E^M (in affine coordinates, eq. (1)). Hint: Either transform the equations to short Weierstrass form and inherit the formulas from there or derive directly via the secant and tangent construction on E^M.

You have two possibilities to answer this question: either write down the formulas or provide a detailed SageMath script (one single file with extension `.py` or `.sage`) with print statements and assert statements, that will compute and validate the formulas, like in the 1st lecture for the affine formulas (file `group_law_short_-weierstrass_affine.sage` in Week 1 on Brightspace), but with your own comments in the file.

Solution 2. We the help of SageMath, we give the formulas in affine coordinates

$$E \colon y^2 = x^3 + Ax^2 + x$$

for points $P(x_1, y_1)$ and $Q(x_2, y_2)$ on the curve.

Negation. Consider $P(x_1, y_1) \in E$. We have $-P = (x_1, -y_1)$.

Addition. Assume $P \neq \pm Q$. If $P = -Q$, the result is $\mathcal{O}$. If $P = Q$, use the doubling formula below. Define the slope λ of the line through P and Q, and find the third intersection point of the line with E. With λ as above, the line equation is $L \colon \lambda(x - x_1) - (y - y_1) = 0 \iff y = \lambda(x - x_1) + y_1$.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \begin{cases} L \colon y = \lambda(x - x_1) + y_1 \\ E \colon y^2 = x^3 + Ax^2 + x \end{cases}$$

We plug in the y-expression from L into E:

$$X^3 - (\lambda^2 - A)X^2 + (2\lambda^2 x_1 - 2\lambda y_1 + 1)X - \lambda^2 x_1^2 + 2\lambda x_1 y_1 - y_1^2 = 0 \tag{3}$$

We know that (x_1, y_1) and (x_2, y_2) are solutions, and there is a third unknown root x_3. Notice that

$$(X - x_1)(X - x_2)(X - x_3) = X^3 - (x_1 + x_2 + x_3)X^2 + (x_1 x_2 + x_1 x_3 + x_2 x_3)X - x_1 x_2 x_3 \tag{4}$$

Hence the coefficients of X^2 in (3) and (4) should be equal, and

$$x_1 + x_2 + x_3 = \lambda^2 - A \iff x_3 = \lambda^2 - A - x_1 - x_2 \ .$$

To compute y_3, consider $L \colon y = \lambda(x - x_1) + y_1$, hence $-y_3 = \lambda(x_3 - x_1) + y_1 \iff y_3 = \lambda(x_1 - x_3) - y_1$.

With SageMath. See the code in the file `group_law_montgomery.sage`. The remainder of (3) mod $(X - x_1)$ is $y_1^2 - x_1^3 - Ax_1^2 - x_1 = f_E(x_1, y_1) = 0$. The quotient is

$$-X^2 + (\lambda^2 - A - x_1)X - \lambda^2 x_1 - Ax_1 - x_1^2 + 2\lambda y_1 - 1 \tag{5}$$

now we simplify with (x_2, y_2) which is a solution. The remainder of (5) mod $(X - x_2)$ is again 0 modulo the curve equation evaluated at (x_2, y_2). The quotient is now linear in X: $-X + \lambda^2 - A - x_1 - x_2 = 0$, and we deduce $x_3 = \lambda^2 - A - x_1 - x_2$. For computing y_3, we use the equation of L as above, and obtain $y_3 = \lambda(x_1 - x_3) - y_1$.

Doubling. This time λ changes, we need the partial derivatives w.r.t. (with respect to) x, resp. y. We have $\frac{\partial f}{\partial x}(x_1, y_1) = -3x_1^2 - 2Ax_1 - 1$, $\frac{\partial f}{\partial x}(x_1, y_1) = 2y_1$, and

$$\lambda = \frac{-\frac{\partial f}{\partial x}(x_1, y_1)}{\frac{\partial f}{\partial y}(x_1, y_1)} = \frac{3x_1^2 + 2Ax_1 + 1}{2y_1} .$$

The line tangent at the curve at (x_1, y_1) has equation

$$L\colon y = \lambda(x - x_1) + y_1 \text{ where } \lambda = \frac{3x_1^2 + 2Ax_1 + 1}{2y_1} .$$

Plugin this y value into E, we get a cubic equation

$$X^3 - (\lambda^2 - A)X^2 + (2\lambda^2 x_1 - 2\lambda y_1 + 1)X - \lambda^2 x_1^2 + 2\lambda x_1 y_1 - y_1^2 = 0 \tag{6}$$

And we know that it has the form

$$(X - x_1)^2(X - x_3) = X^3 - (x_3 + 2x_1)X^2 + (2x_3x_1 + x_1^2)X - x_1^2 x_3 = 0$$

hence we solve equality for the coefficients of the X^2 term:

$$x_3 + 2x_1 = \lambda^2 - A \iff x_3 = \lambda^2 - A - 2x_1 .$$

We obtain y_3 as before thanks to the line equation $L\colon y = \lambda(x - x_1) + y_1$, with x_3, we get $y_3 = \lambda(x_1 - x_3) - y_1$.

Wrapping up, the group law on E^M with $P(x_1, y_1)$, $Q(x_2, y_2)$ is

- $-P = (x_1, -y_1)$
- $P + Q = \mathcal{O}$ if $P = -Q$,
- if $P \neq -Q$, (including $P \neq (x_1, 0)$) then $P + Q$ is (x_3, y_3) where

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 - A \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases} \text{ with } \lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq \pm Q; \\ \frac{3x_1^2 + 2Ax_1 + 1}{2y_1} & \text{if } P = Q. \end{cases}$$

Question 3. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on E^M. Let $P_1 + P_2 = (x_3, y_3)$ and $P_1 - P_2 = (x_4, y_4)$.

Assume that $x_1 \neq x_2$, $x_1 \neq 0$ and $x_2 \neq 0$. Show that

$$x_3(x_1 - x_2)^2 = \frac{(x_2 y_1 - x_1 y_2)^2}{x_1 x_2} \tag{7}$$

$$x_4(x_1 - x_2)^2 = \frac{(x_2 y_1 + x_1 y_2)^2}{x_1 x_2} \tag{8}$$

$$x_3 x_4 (x_1 - x_2)^2 = (x_1 x_2 - 1)^2 \tag{9}$$

Solution 3. The curve has equation $y^2 = x^3 + Ax^2 + x$. The line through P_1 and P_2 has slope $\lambda = (y_1 - y_2)/(x_1 - x_2)$. This line has equation

$$L\colon y = \lambda(x - x_1) + y_1 = \lambda x + y_1 - \lambda x_1, \text{ where } \lambda = \frac{y_1 - y_2}{x_1 - x_2}.$$

We plug into E^M:

$$\begin{aligned} E^M \cap L \quad &: \quad y^2 = ((\lambda x) + (y_1 - \lambda x_1))^2 = x^3 + Ax^2 + x \\ &: \quad x^3 + Ax^2 + x - \lambda^2 x^2 - \lambda x(y_1 - \lambda x_1) - (y_1 - \lambda x_1)^2 = 0 \end{aligned}$$

Because x_1, x_2, and x_3 are the three roots of this cubic polynomial, their product is the negative of the constant coefficient, and

$$\begin{aligned} x_1x_2x_3 &= (y_1-\lambda x_1)^2 \\ x_3 &= \frac{(y_1-\lambda x_1)^2}{x_1x_2} \text{ where we assume that } x_1x_2\neq 0 \\ x_3(x_1-x_2)^2 &= \frac{(y_1(x_1-x_2)-(y_1-y_2)x_1)^2}{x_1x_2} \text{ where } \lambda=\frac{y_1-y_2}{x_1-x_2} \\ x_3(x_1-x_2)^2 &= \frac{(-y_1x_2+y_2x_1)^2}{x_1x_2}=\frac{(y_1x_2-y_2x_1)^2}{x_1x_2} \end{aligned}$$

For x_4, we do the same strategy but with $-y_2$ instead of y_2 and obtain

$$x_4(x_1-x_2)^2 = \frac{(y_1x_2+y_2x_1)^2}{x_1x_2}$$

For the third equation, we will multiply together the two other ones, but first we rewrite

$$\begin{aligned} x_3(x_1-x_2)^2 &= \frac{(x_1x_2(y_1/x_1-y_2/x_2))^2}{x_1x_2}=x_1x_2\left(\frac{y_1}{x_1}-\frac{y_2}{x_2}\right)^2 \\ x_4(x_1-x_2)^2 &= \frac{(x_1x_2(y_1/x_1+y_2/x_2))^2}{x_1x_2}=x_1x_2\left(\frac{y_1}{x_1}+\frac{y_2}{x_2}\right)^2 \end{aligned}$$

Their product is

$$x_3x_4(x_1-x_2)^4 = x_1^2x_2^2\left(\left(\frac{y_1}{x_1}\right)^2-\left(\frac{y_2}{x_2}\right)^2\right)^2$$

Now we use E^M equation to simplify:

$$E^M: y^2=x^3+Ax^2+x,\ x\neq 0 \implies \frac{y^2}{x^2}=x+A+\frac{1}{x}$$

So with

$$\begin{cases} \frac{y_1^2}{x_1^2}=x_1+A+\frac{1}{x_1} \\ \frac{y_2^2}{x_2^2}=x_2+A+\frac{1}{x_2} \end{cases} \implies \frac{y_1^2}{x_1^2}-\frac{y_2^2}{x_2^2}=x_1-x_2+\frac{1}{x_1}-\frac{1}{x_2}\ ,$$

$$\frac{y_1^2}{x_1^2}-\frac{y_2^2}{x_2^2}=x_1-x_2+\frac{x_2-x_1}{x_1x_2}=(x_1-x_2)\left(1-\frac{1}{x_1x_2}\right)$$

Finally,

$$\begin{aligned} x_3x_4(x_1-x_2)^4 &= x_1^2x_2^2\left((x_1-x_2)\left(1-\frac{1}{x_1x_2}\right)\right)^2 \\ x_3x_4(x_1-x_2)^2 &= \left(x_1x_2\left(1-\frac{1}{x_1x_2}\right)\right)^2 \\ x_3x_4(x_1-x_2)^2 &= (x_1x_2-1)^2\ . \end{aligned}$$

Long version, but it is better to write the above shorter solution.

We start from

$$y_1^2=x_1(x_1^2+Ax_1+1) \iff y_1^2/x_1=x_1^2+Ax_1+1 \text{ as } x_1\neq 0 \tag{10}$$

$$y_2^2=x_2(x_2^2+Ax_2+1) \iff y_2^2/x_2=x_2^2+Ax_2+1 \text{ as } x_2\neq 0 \tag{11}$$

The difference of the two equations is

$$(10)-(11)=\frac{y_1^2x_2-y_2^2x_1}{x_1x_2}=x_1^2+Ax_1-x_2^2-Ax_2=(x_1-x_2)(x_1+x_2+A) \tag{12}$$

Now we consider $x_3(x_1-x_2)^2$, where $x_3 = \lambda^2-x_1-x_2-A$, and $\lambda = (y_2-y_1)/(x_2-x_1)$.

$$x_3(x_1-x_2)^2 = \left(\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2 - A\right)(x_1-x_2)^2 \tag{13}$$

$$=(y_2-y_1)^2 - (x_1+x_2+A)(x_1-x_2)^2 \tag{14}$$

$$=\frac{(y_2^2-2y_1y_2+y_1^2)x_1x_2}{x_1x_2} - \frac{(y_1^2x_2-y_2^2x_1)(x_1-x_2)}{x_1x_2} \tag{15}$$

$$=\frac{y_1^2x_2^2+y_2^2x_1^2-2y_1y_2x_1x_2}{x_1x_2} \tag{16}$$

$$=\frac{(y_1x_2-y_2x_1)^2}{x_1x_2} = \frac{(x_2y_1-x_1y_2)^2}{x_1x_2} . \tag{17}$$

For the second equation to prove, actually we change y_2 into $-y_2$, and we obtain directly the solution.

For the third equation, first we re-write

$$x_3(x_1-x_2)^2 = \left(\frac{y_1}{x_1} - \frac{y_2}{x_2}\right)^2 x_1x_2,\ \ x_4(x_1-x_2)^2 = \left(\frac{y_1}{x_1} + \frac{y_2}{x_2}\right)^2 x_1x_2$$

hence their product is

$$x_3x_4(x_1-x_2)^4 = \left(\frac{y_1^2}{x_1^2} - \frac{y_2^2}{x_2^2}\right)^2 x_1^2x_2^2 \tag{18}$$

and from (10) and (11),

$$y_1^2/x_1^2 = x_1 + A + 1/x_1,\ \ x_1 \neq 0 \tag{19}$$

$$y_2^2/x_2^2 = x_2 + A + 1/x_2,\ \ x_2 \neq 0 \tag{20}$$

their difference is

$$\frac{y_1^2}{x_1^2} - \frac{y_2^2}{x_2^2} = x_1 - x_2 + \frac{1}{x_1} - \frac{1}{x_2} = x_1 - x_2 + \frac{x_2-x_1}{x_1x_2} = (x_1-x_2)\frac{x_1x_2-1}{x_1x_2}$$

So finally,

$$x_3x_4(x_1-x_2)^2 = \frac{x_1^2x_2^2}{(x_1-x_2)^2}\frac{(x_1-x_2)^2(x_1x_2-1)^2}{(x_1x_2)^2} \tag{21}$$

$$=(x_1x_2-1)^2 \tag{22}$$

Question 4. Show that (9) remains valid also for the special cases $x_1 = 0$ or $x_2 = 0$.

Solution 4. Assume $x_1 = 0$, hence $y_1 = 0$, but $x_2, y_2 \neq 0$. Then $\lambda = y_2/x_2$, $x_3 = \lambda^2 - x_2 - A = (y_2^2 - x_2^3 - Ax_2^2)/x_2^2$ and at the numerator, we recognize the curve equation up to a term $-x_2$, consequently $x_3 = x_2/x_2^2 = 1/x_2$. We obtain the same for x_4 (starting with $-y_2$ instead of y_2, the sign disappears in the square). Hence

$$x_3x_4 = \frac{1}{x_2^2} \iff = x_3x_4x_2^2 = 1$$

which is (9) with $x_1 = 0$, $x_2 \neq 0$. If $x_2 = y_2 = 0$ but $x_1 \neq 0$, then we obtain the same with x_1 instead of x_2: $x_3x_4x_1^2 = 1$.

Question 5. For $P_1 = P_2$ show that

$$4x_1x_3(x_1^2 + Ax_1 + 1) = (x_1^2-1)^2 . \tag{23}$$

Remark 1. Note that (9) and (23) do not involve y_1 or y_2 and that we can use the same formulas in all cases.

Solution 5. Now $P_1 = P_2$ and $\lambda = (3x_1^2 + 2Ax_1 + 1)/(2y_1)$, $x_3 = \lambda^2 - 2x_1 - A$. Note that $4x_1(x_1^2 + Ax_1 + 1) = 4y_1^2$ from the curve equation.

$$\begin{aligned}
&4x_1x_3(x_1^2 + Ax_1 + 1) = 4y_1^2\left(\lambda^2 - 2x_1 - A\right) \\
=&(3x_1^2 + 2Ax_1 + 1)^2 - (2x_1 + A)(4x_1^3 + 4Ax_1^2 + 4x_1) \\
=&9x_1^4 + 4A^2x_1^2 + 12Ax_1^3 + 1 + 6x_1^2 + 4Ax_1 \\
&\quad - (8x_1^4 + 8Ax_1^3 + 8x_1^2 + 4Ax_1^3 + 4A^2x_1^2 + 4Ax_1) \\
=&x_1^4 - 2x_1^2 + 1 = (x_1^2 - 1)^2 \ .
\end{aligned}$$

2. Divisibility by 4 of $\#E^M(\mathbb{F}_p)$

The following results show that 4 is always a divisor of $\#E^M(\mathbb{F}_p)$. This implies that not all elliptic curves can be transformed to Montgomery form E^M over $\mathbb{F}_p$.

Question 6.

- Show that E^M has exactly three points of order 2 if the discriminant $A^2 - 4$ is a quadratic residue.
- Show that E^M has exactly one point of order 2, which is $(0, 0)$, if the discriminant $A^2 - 4$ is a quadratic non-residue.
- The point $(1, \pm\gamma)$ has order 4 if $A + 2$ is a quadratic residue, where γ is one of the quadratic roots of $A + 2$.
- The point $(-1, \pm\delta)$ has order 4 if $A - 2$ is a quadratic residue, where δ is one of the quadratic roots of $A - 2$.

Solution 6. The points of order two are of the form $P(x_1, 0)$ hence we compute the roots of $x_1(x_1^2 + Ax_1 + 1) = 0$, there are $x_1 = 0$ and x_1', x_1'' such that $x_1' = (-A + \sqrt{A^2 - 4})/2$, $x_1'' = (-A - \sqrt{A^2 - 4})/2$. Taking into account the point at infinity $\mathcal{O}$, there are always two 2-torsion points (whose order divides 2) on E^M: $\{\mathcal{O}, (0, 0)\}$ and when $\sqrt{A^2 - 4}$ exists in the field of definition, that is, $A^2 - 4$ is a square (or a quadratic residue), then there are two more points of order two, hence there are four 2-torsion points, in this case the order of the curve is a multiple of 4. If $A^2 - 4$ is not a square, x_1', x_1'' are not defined over the field, and there are no extra points of order two.

Consider $P(1, \pm\gamma)$ where $\gamma = \sqrt{A + 2}$. We compute $2P$ and expect to find a 2-torsion point of the form $(x_3, 0)$. We start with $\lambda = (3x_1^2 + 2Ax_1 + 1)/(2y_1) = \pm(2 + A)/\gamma = \pm\gamma^2/\gamma = \pm\gamma$. Then $x_3 = \lambda^2 - 2x_1 - A = \gamma^2 - 2 - A = 0$, and it follows that $y_3 = \lambda(x_1 - x_3) - y_1 = \pm\gamma - (\pm\gamma) = 0$. We checked that $2P = (0, 0)$ hence $P(1, \pm\gamma)$ are two points of order 4.

Consider $P(-1, \pm\delta)$ where $\delta = \sqrt{A - 2}$. We compute $2P$ and expect to find a 2-torsion point of the form $(x_3, 0)$. We start with $\lambda = (3x_1^2 + 2Ax_1 + 1)/(2y_1) = \pm(2 - A)/\delta = \pm(-\delta^2)/\delta = \mp\delta$. Then $x_3 = \lambda^2 - 2x_1 - A = \delta^2 + 2 - A = 0$, and it follows that $y_3 = \lambda(x_1 - x_3) - y_1 = \mp\delta(-1) - (\pm\delta) = 0$. We checked that $2P = (0, 0)$ hence $P(-1, \pm\delta)$ are two points of order 4.

Question 7. Show that $\#E^M(\mathbb{F}_p)$ is always divisible by 4.

Solution 7. The curve has order multiple of 4 if there are four 2-points ($\mathcal{O}$ and three points of order two), or if there are $\mathcal{O}$, one point of order two and (at least) two points of order 4.

We know that there are at least two 2-torsion points, namely $\{P_2(0, 0), \mathcal{O}\}$. With the notation $\gamma = \sqrt{A + 2}$, $\delta = \sqrt{A - 2}$, and $\gamma\delta = \sqrt{A^2 - 4}$, the two other points of order two are $((-A \pm \gamma\delta)/2, 0)$, and the points of order 4 are $P_4(-1, \delta), -P_4$ and $Q_4(1, \gamma), -Q_4$, where $2P_4 = P_2$, $2Q_4 = P_2$. Note that $P_4 + P_2 = P_4 + 2P_4 = 3P_4 = -P_4$ and similarly $Q_4 + P_2 = Q_4 + 2Q_4 = 3Q_4 = -Q_4$.

Now a reasoning about quadratic residues is required.

- If $A+2$ is a square, $\pm P_4$ are rational and the curve order is multiple of 4.
- If $A-2$ is a square, $\pm Q_4$ are rational and the curve order is multiple of 4.
- If none of $A-2, A+2$ is a square, there are no points of order 4, but in that case, the product of the two non-quadratic-residues $(A+2)(A-2)$ is a square, $\sqrt{A^2-4}$ is rational, and the two other points of order two are defined.

We conclude that the curve order is always multiple of 4.

3. Curve25519

Let $p = 2^{255} - 19$ and let E^M have the affine equation

$$E^M : y^2 = x^3 + 486662x^2 + x \ .$$

See `http://cr.yp.to/ecdh.html#curve25519-paper` and `https://en.wikipedia.org/wiki/Curve25519`.

Question 8. This question involves SageMath.

With SageMath, check that p is a prime then define the finite field $\mathbb{F}_p$ in SageMath.

Check that E^M is an elliptic curve in Montgomery form. Determine a point in $E(\mathbb{F}_p)$ of order 4. Determine $\#E^M(\mathbb{F}_p)$ (find the appropriate function call in SageMath, remember that you can use the tabulation key to show you the methods associated to an instance of a class) and compare the number with $p+1$: is the curve supersingular or ordinary? Show that $\#E^M(\mathbb{F}_p)$ has a large subgroup of prime order.

Some hints on elliptic curves in SageMath: `https://doc.sagemath.org/html/en/constructions/elliptic_curves.html`.

Solution 8.

```
p = ZZ(2**255-19)
p.is_prime()
Fp = GF(p)
A = Fp(486662)
B = Fp(1)
EM = EllipticCurve([0,A,0,B,0]) # it will throw an exception if EM is singular
# points of order 4
if (A-2).is_square():
    delta = sqrt(A-2)
    P4 = EM((-1, delta))
    assert 2*P4 == EM((0,0))
    print("P_4(-1, sqrt(A-2)) is defined")
if (A+2).is_square():
    gamma = sqrt(A+2)
    P4 = EM((1, gamma))
    assert 2*P4 == EM((0,0))
    print("P_4(1, sqrt(A+2)) is defined") # this one is Fp-rational
if (A**2-4).is_square():
    alpha = sqrt(A**2-4)
    Q2 = EM((-A + alpha)/2, 0)
    R2 = EM((-A - alpha)/2, 0)
    print("Q_2((-A+sqrt(A^2-4))/2, 0) is defined")
    print("R_2((-A-sqrt(A^2-4))/2, 0) is defined")
# two options for computing the order: method EM.order() or with the trace
orderE = EM.order()
assert orderE % 4 == 0
r = orderE // 8 # actually the curve order is multiple of 8
```

```
assert r.is_prime() # the curve order is 8 times a large prime of 253 bits
r.nbits()
tr = EM.trace_of_frobenius() # alternative
orderEtr = p + 1 - tr
assert orderE == orderEtr
# base point:
x0 = Fp(9)
y02 = x0^3 + A*x0^2 + B*x0
y0 = y02.sqrt()
P = EM((x0, y0))
assert r*P == EM(0)
EM.is_supersingular() # the curve is not supersingular
assert gcd(tr, p) == 1 # alternative: the trace is coprime to the characteristic p
```

4. Comments on SageMath code.

What is the problem with this statement?

```
P4 = EM((Fp(1), (A+Fp(2)).sqrt()))
assert P4.order() == 4
```

The while loop can take a lot of time. Alternatively, `P4.order()` computes the discrete logarithm of $P4$ on the curve. The help with the question mark: `P4.order?` gives info on the function: it calls `ellorder` from PARI. IN PARI documentation, one finds `https://pari.math.u-bordeaux.fr/dochtml/html/Elliptic_curves.html#ellorder` so first this call **computes the curve order and factor it, then tries the different possibilities**. If the curve has a large composite order, factoring it will take minutes, or even hours! If you only want to check that the points has order 4, checks that

```
assert 4*P4 == EM(0) and 2*P4 != EM(0)
# timing:
time P4.order()
CPU times: user 39.5 ms, sys: 0 ns, total: 39.5 ms
Wall time: 39.7 ms
def check(Q):
    return (4*Q == EM(0) and 2*Q != EM(0))
time check(P4)
CPU times: user 238 µs, sys: 24 µs, total: 262 µs
Wall time: 267 µs
```

What is the problem with this statement?

```
# finding a generator G of order r = EM.order()//8
EMorder = EM.order()
G = EM.random_element()
while(G.order() != r):
    G = EM.random_element()
```

The while loop can take a lot of time. Alternatively, uses

```
EMorder = EM.order()
G0 = EM.random_element()
G = 8*G0 # clear cofactor
while(G == EM(0)):
    G0 = EM.random_element()
    G = 8*G0
```

But the way to generate G_0 is randomized, and one can ask what kind of randomness was used. Instead, defines a deterministic procedure.

```
EMorder = EM.order()
x0 = Fp(3) # x0 = 0 -> point of order 2, x0=1 -> point of order 4, start at 2
y02 = x0**3 + A*x0**2 + x0
while not y02.is_square():
    x0 = x0+1
    y02 = x0**3 + A*x0**2 + x0
y0 = y02.sqrt()
G0 = EM((x0,y0))
while not r*G0 == EM(0):
    x0 = x0+1
    y02 = x0**3 + A*x0**2 + x0
    while not y02.is_square():
        x0 = x0+1
        y02 = x0**3 + A*x0**2 + x0
    y0 = y02.sqrt()
    G0 = EM((x0,y0))
# there is no do-while loop in Python...
```

We get $G(9, \sqrt{9^3 + A \cdot 9^2 + 9})$.

Why is it not a good idea to ask for `EM.oder().factor()`? It can take hours if this number has medium-size factors (for example, if it is a composite number made of two primes of roughly the same size, it can take hours). We can instead look for the cofactor.

```
C = prod(prime_range(10**6))
order = EM.order()
N = order
g = gcd(C, N)
cofactor = 1
while g > 1:
    cofactor = cofactor * g
    N = N // g
    g = gcd(g, N)
assert cofactor * N == order and N.is_prime()
```

About the order, and the prime subgroup. The cofactor is 8. What's wrong with this statement:

```
r = EM.order()/8
r.is_prime()
False
```

The result is not an integer (Integer) but a rational in SageMath, (and in Python 3), instead, use Euclidean division:

```
r = EM.order()//8
r.is_Prime()
True
```

References

[1] Peter L. Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–264, 1987.

[2] Katsuyuki Okeya, Hiroyuki Kurumatani, and Kouichi Sakurai. Elliptic curves with the montgomery-form and their cryptographic applications. In *Public Key Cryptography, Third International Workshop on Practice and Theory in Public Key Cryptography, PKC 2000, Melbourne, Victoria, Australia, January 18-20, 2000*, volume 1751 of *Lecture Notes in Computer Science*, pages 238–257. Springer, 2000.