Elliptic curves, number theory and cryptography –
Elliptiske kurver, talteori og kryptographi

1. handin – 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 $p \neq 2$ and let $\mathbb{F}_p$ be the finite field with p elements. Let $A \in \mathbb{F}_p$ and consider the equations:

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

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

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.

Hint: you can use the fact that the j-invariant should be well-defined, and its formula is $j(E^M) = 256\frac{(A^2-3)^3}{A^2-4}$. Alternatively, you can check the condition so that $f(x) = x^3 + Ax^2 + x$ has no multiple root, but three distinct simple roots (in that case the curve is smooth).

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.

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 $P_1 - P_2 = (x_4, y_4)$.

Question 3. Assume that $x_1 \neq x_2$, $x_1 \neq 0$ and $x_2 \neq 0$. Show that

$$x_3(x_1 - x_2)^2 = \frac{(x_2 y_1 - x_1 y_2)^2}{x_1 x_2} \tag{3}$$

$$x_4(x_1 - x_2)^2 = \frac{(x_2 y_1 + x_1 y_2)^2}{x_1 x_2} \tag{4}$$

$$x_3 x_4 (x_1 - x_2)^2 = (x_1 x_2 - 1)^2 \tag{5}$$

Hint: for (3) and (4), you can use the same strategy as Exercise 2.1 in Washington's book: note that the constant coefficient of a monic cubic polynomial is the negative of the product of the roots, that is, if $f(x) = x^3 + a_2 x^2 + a_1 x + a_0 = (x - x_1)(x -$

$x_2)(x - x_3)$, then $x_1x_2x_3 = -a_0$. Use this property to obtain the formula for x_3, resp. x_4.

Hint: for (5), first rewrite (3) as $x_3(x_1 - x_2)^2 = x_1x_2\left(\frac{y_1}{x_1} + \frac{y_2}{x_2}\right)^2$ and equivalently for (4), then multiply (3) to (4). Observe that dividing the curve equation by x^2 if it is non-zero, then one obtains $y^2/x^2 = x + A + 1/x$. Use that to deduce that

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

Conclude.

Question 4. Show that (5) remains valid also for the special cases $x_1 = 0$ or $x_2 = 0$.

Question 5. For $P_1 = P_2$ show that

$$4x_1x_3(x_1^2 + Ax_1 + 1) = (x_1^2 - 1)^2 . \tag{6}$$

Remark 1. Note that (5) and (6) do not involve y_1 or y_2 and that we can use the same formulas in all cases.

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 $A - 2$.

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

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.