Master CSI, AGTN/ALGANT

2019-2020

Courbes elliptiques — 4TMA902U

Mid Term Exam — October 25, 2019

1h30, Documents are not allowed, Answer the two parts on separate sheets

D. Robert's Part

1 Let E be the curve defined over $\mathbf{F}_{11}$ by the long Weierstrass equation $y^2 + xy = x^3 + x + 1$.

(a) Find a short Weierstrass equation $E' : y^2 = x^3 + ax + b$ for E.

(b) Show that E is an elliptic curve.

(c) Let $P = (3, 10)$. Check that P is a point on E.

(d) Recall the formulae for the addition law on E′.

(e) Compute 2P. (Hint: use the change of variable to E′).

2 Let $E : x^2 + y^2 = 1 + dx^2y^2$ be a curve over a field k of characteristic different from 2, such that d is different from 0 or 1.

(a) Show that E is a smooth affine curve.

(b) Show that E has two points at infinity.

(c) Show that the points at infinity are not smooth.

We admit that there is a change of formula from E to an elliptic curve, defined everywhere apart from the two points at infinity. From this we deduce that there is an addition law on the affine points:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

(e) Show that we can rewrite the addition law as

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_1 + x_2y_2}{x_1x_2 + y_1y_2}, \frac{x_1y_1 - x_2y_2}{x_1y_2 - y_1x_2} \right).$$

(f) Show that $0_E = (0, 1)$ and that $-(x, y) = (-x, y)$.

(g) Show that $P = (1, 0)$ is a point of 4-torsion.

(h) Show that if we work over $k = \mathbf{F}_q$ and d is not a square in $\mathbf{F}_q$, then the addition law is always defined, meaning that the denominators are never zero.
Hint: let $\epsilon = dx_1y_1x_2y_2$ and suppose by contradiction that $\epsilon = \pm 1$. Show that $dx_1^2y_1^2(x_2^2+y_2^2) = x_1^2 + y_1^2$ and then that $(x_1 + \epsilon y_1)^2 = dx_1^2y_1^2(x_2 + y_2)^2$. Conclude that d is a square.

(i) Now suppose that $k = \mathbb{R}$ and $d = 0$, so we are working on the real circle $x^2 + y^2 = 1$. Show that the addition law is still valid.

(j) Still when $d = 0$ and $k = \mathbb{R}$, writing $(x_1, y_1) = (\sin\theta_1, \cos\theta_1)$ and $(x_2, y_2) = (\sin\theta_2, \cos\theta_2)$ (warning: here we exchange the usual roles of x and y), then show that $(x_1, y_1) + (x_2, y_2) = (\sin(\theta_1 + \theta_2), \cos(\theta_1 + \theta_2))$. So we recover the "standard angle addition" on the circle.

G. Castagnos' Part

$\boxed{3}$ We recall the ECDSA signature scheme:

- **Global Public Parameters:**

  P a point of order n of an elliptic curve E defined over $\mathbf{F}_p$, $H : \{0,1\}^* \to \{1, \dots, n-1\}$ a cryptographic hash function

- **Key Generation:** $pk := Q := xP$ with x random $0 < x < n$, $sk := x$

- **Signing a message m with the key x:**

  r random, $0 < r < n$, $R := (x_R, y_R) := rP$, If $x_R \equiv 0 \pmod{n}$, restart with another r.

  $s :\equiv r^{-1}(x(x_R \mod n) + H(m)) \pmod{n}$. If $s \equiv 0 \pmod{n}$, restart with another r.

  The signature is $\sigma := (\sigma_1, \sigma_2) := (x_R \mod n, s)$.

- **Verifying a signature (σ_1, σ_2) of m with the key $pk = Q$**

  Verify that Q is on the curve, and that Q has order n and that $1 < \sigma_i < n$, for $i = 1, 2$.

  $u_1 :\equiv H(m)\sigma_2^{-1} \pmod{n}$; $u_2 :\equiv \sigma_1\sigma_2^{-1} \pmod{n}$; $(x_1, y_1) := u_1P + u_2Q$

  Signature is correct if $\sigma_1 \equiv x_1 \pmod{n}$

(a) What is the goal of a signature algorithm? Why using a signature algorithm with elliptic curves instead of a similar algorithm with finite fields?

(b) In this question, we consider a bad implementation of ECDSA where r is not random but fixed with an unknown value. Suppose that you have two different messages m and m' and their signatures σ and σ' computed with this implementation with the same secret key x. Show that you can recover x.

(c) Suppose in this question, that you have found a message m such that $H(m) = 0$. Show how it is possible to compute efficiently (in polynomial time) a valid signature with ECDSA of m without knowing the secret key sk.

(d) Suppose in this question that in the ECDSA scheme, H is replaced by the identity : $H = Id : \{1, \dots, n-1\} \to \{1, \dots, n-1\}$. Show that it is possible to compute efficiently (in polynomial time) a signature of an uncontrolled message $m \in \{1, \dots, n-1\}$ without knowing the secret key (Hint: set $R = aP + bQ$ for some a, b and then choose well the values of s and m).

$\boxed{4}$ Let $(G, \times)$ be a cyclic group of prime order n. Let g be a generator of G. Let a, b and x be three integers such that $1 < a < x < b < n$. We denote $h = g^x$.

Give a detailed algorithm (in pseudo code) that outputs x given G, n, a, b, g, h, knowing that $a < x < b$. This algorithm must use at most $\mathcal{O}(\sqrt{b-a})$ exponentiations in the group G and storage of $\mathcal{O}(\sqrt{b-a})$ elements of the group G in memory. Explain why your algorithm gives a correct output.