Courbes elliptiques — 4TMA902U

Responsables : G. Castagnos, D. Robert

Mid Term Exam — October 23, 2020

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

D. Robert's Part

1

(a) Let E be the curve $y^2 = x^3 - 1$ over $\mathbf{F}_7$. Check that E is an elliptic curve.

(b) Recall the Hasse-Weil bound on $\#E(\mathbf{F}_q)$.

(c) Give the list of all points in $E(\mathbf{F}_7)$ and compare with the Hasse-Weil bound.

(d) Recall the formula for the addition law of two points $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ in an elliptic curve (given by a short Weierstrass equation).

(e) Let $P = (1, 0)$ and $Q = (2, 0)$. Show that $P, Q \in E(\mathbf{F}_7)$ and compute $2P$, $2Q$, $P + Q$.

(f) Determine to which abelian group $E(\mathbf{F}_7)$ is isomorphic to.

(g) Give the list of all squares in $\mathbf{F}_7$ and show that -1 is not a square.

(h) Let E' be the curve $-y^2 = x^3 - 1$. Use a change of variable to show that E' is isomorphic to the curve $y^2 = x^3 + 1$ and is an elliptic curve.

(i) Show that if $z \in \mathbf{F}_7^*$, then either z is a square, or $-z$ is a square (and both cannot be squares at the same time).

(j) Deduce that $\#E(\mathbf{F}_7) + \#E'(\mathbf{F}_7) = 2 \times (7 + 1) = 16$. From this relation, compute $\#E'(\mathbf{F}_7)$.

(k) Recall the definition of the j-invariant of an elliptic curve. Under which conditions do we have $j(E_1) = j(E_2)$ for two elliptic curves E_1, E_2 defined over a field k?

(l) We compute with Sage that $j(E) = j(E') = 0$. What does this mean about E and E'?

(m) Show that E and E' cannot be isomorphic over $\mathbf{F}_7$.

(n) Give an isomorphism between E and E' over $\mathbf{F}_{7^2}$.

2 Let $E : y^2 = x^3 + 162x + 729$ be a curve over $\mathbf{Q}$. Remark that $162 = 2 \cdot 3^4$ and $729 = 3^6$.

(a) Recall the definition of the discriminant Δ_E of an elliptic curve.

(b) We compute with Sage that $\Delta_E = -501680304 = -2^4 \cdot 3^{12} \cdot 59$.

(c) Show that E is an elliptic curve over $\mathbf{Q}$.

(d) If p is a prime number, we denote by $E_p : y^2 = x^3 + (162 \mod p)x + (729 \mod p)$ the curve E reduced modulo p. For which primes p is the curve E_p not an elliptic curve? When E_p is an elliptic curve, we say that p is a prime of *good reduction*. Otherwise we say that p is of *bad reduction*.

(e) For $p = 2$ and $p = 3$, give an exemple of a non smooth point P on E_p.

(f) Recall what are the isomorphisms between short Weierstrass equations.

(g) Show that E is isomorphic to the curve $E' : y^2 = x^3 + 2x + 1$.

(h) We compute with Sage that $\Delta_{E'} = -2^4 \cdot 59$. What can we say about the primes of bad reduction of E'?

(i) Show that there is no isomorphism from E' to another curve E" in short Weierstrass form such that $|\Delta_{E''}| < |\Delta_{E'}|$. We say that E' is the minimal model of E. (Warning: sometime the minimal model is given by a long Weierstrass equation, we admit that this is not the case here.)

(j) Show that if p is a prime of good reduction, the map $E(\mathbf{Q}) \to E_p(\mathbf{F}_p)$ is well defined and is a group morphism.

(k) The Nagell-Lutz theorem states that if $P \in E(\mathbf{Q})$ is a point of torsion, then $P = (x, y)$ is given by integer coordinates ($x, y \in \mathbf{Z}$). Deduce that if p is a prime of good reduction, $E_{\text{tors}}(\mathbf{Q}) \to E_p(\mathbf{F}_p)$ is injective.

(l) We compute $\#E_5(\mathbf{F}_5) = 7$, $\#E_7(\mathbf{F}_7) = 5$. Deduce that $E_{\text{tors}}(\mathbf{Q}) = \{0_E\}$.

(m) Let $P = (0, 27) \in E(\mathbf{Q})$. We compute that $4P = (-63/16, 351/6)$. Deduce that P is a point of infinite order.

(n) We compute that $7P = (-4784/2025, -1663111/91125)$, and $5P = (1656/49, -72603/343)$. Explain why we were expecting that we would get coordinates with denominators divisible by 5 and 7 respectively.

G. Castagnos' Part

$\boxed{3}$ Let $(G, \times)$ be a cyclic group of prime order n. We denote by g a generator of G and by ℓ the number of bits of n. Let ω be an integer with $1 \leqslant \omega \leqslant \ell$. In the following, we will suppose that ω is even. Let x be an integer with $1 < x < n$. We suppose that the Hamming weight of x is equal to ω, which means that the number of times that 1 appears in the binary decomposition of x is exactly ω. We denote $h = g^x$.

(a) Show that we can write $x = x_1 + x_2$ with x_1 and x_2 two integers of Hamming weight $\omega/2$.

(b) Deduce from that an algorithm (in pseudo code) that outputs x given G, n, g, h and ω and which needs $\mathcal{O}\left(\binom{\ell}{\omega/2}\right)$ exponentiations in the group G and stores in memory $\mathcal{O}\left(\binom{\ell}{\omega/2}\right)$ group elements. Prove that your algorithm returns the correct solution with the expected complexity.

$\boxed{4}$ Let p be a prime number and let E be an elliptic curve over $\mathbf{F}_p$. Let q be a prime number and let us suppose that there exits $\mathrm{P} \in \mathrm{E}(\mathbf{F}_p)$ a point of order q. Denote $\mathrm{G} = \langle \mathrm{P} \rangle$ the subgroup of $\mathrm{E}(\mathbf{F}_p)$ generated by P. We recall the Elgamal asymmetric encryption scheme in G using additive notation. The secret key in an element x with $1 \leqslant x \leqslant q$, the public key is composed of P, $\mathrm{Q} = x\mathrm{P}$ and q. To encrypt a point $\mathrm{M} \in \mathrm{G}$ with this public key, pick a random r with $1 \leqslant r \leqslant q$ and the ciphertext is $c = (c_1, c_2) = (r\mathrm{P}, \mathrm{M} + r\mathrm{Q})$.

(a) Give a decryption algorithm (in pseudo code) for the Elgamal scheme in G.

In the following, we denote by c an encryption of M. We suppose that $\mathrm{Card}\,\mathrm{E}(\mathbf{F}_p) > q$, that $\mathrm{M} = (x_\mathrm{M}, y_\mathrm{M})$ is an element of $\mathrm{E}(\mathbf{F}_p)$, and that the order of M is **not** q.

(b) In this question, we suppose that $1 < x_\mathrm{M} < 2^k$, where k is an integer much smaller than the bit length of p. Give an algorithm (in pseudo code) that tries to recover M from c using at most 2^k exponentiations in $\mathrm{E}(\mathbf{F}_p)$. Explain why your algorithm gives a correct output.

(c) In this question, we suppose that M is the sum of two points with small x coordinates: $\mathrm{M} = \mathrm{M}_1 + \mathrm{M}_2$ and for $i \in \{1, 2\}$, $\mathrm{M}_i \in \mathrm{E}(\mathbf{F}_p)$, $\mathrm{M}_i = (x_{\mathrm{M}_i}, y_{\mathrm{M}_i})$ and $1 < x_{\mathrm{M}_i} < 2^k$. Give an algorithm (in pseudo code) that tries to recover M from c, by storing at most 2^k elements of $\mathrm{E}(\mathbf{F}_p)$ in memory and using at most 2^{k+1} exponentiations in $\mathrm{E}(\mathbf{F}_p)$. Explain why your algorithm gives a correct output.