Université de Bordeaux
Master Mathématiques et Applications
Année 2016-2017

Algorithmique Arithmétique

15 décembre 2016

Documents allowed
The exercises are independent
The three parts will be evaluated on the same number of points

Part 1 : Number theory

Let E be an elliptic curve defined over the finite field $\mathbb{Z}/p\mathbb{Z}$, and let $P \in E(\mathbb{Z}/p\mathbb{Z})$ be a point on E. let N be a positive number and let $N = a_0 + 2a_1 + \cdots + 2^k a_k$, with $a_i \in \{0, 1\}$, be its binary expansion.

1. Recall in this context the fast algorithm to compute $NP = \underbrace{P + \cdots + P}_{N}$, refered to here as *double and add*. Precisely compute the number of additions in $E(\mathbb{Z}/p\mathbb{Z})$ that this algorithm requires, in terms of the number of 0 and 1 in the binary expansion of N.
2. Explain why a substraction in $E(\mathbb{Z}/p\mathbb{Z})$ is essentially not more costly than an addition. In the following, we call 'operation' either an addition or a substraction in $E(\mathbb{Z}/p\mathbb{Z})$.
3. Let $N = 1 + 2 + \cdots + 2^k$. Noticing that $N = 2^{k+1} - 1$, give a method that allows to compute NP with $k + 2$ operations, and compare with *double and add*.
4. Inspired by the previous question, show that one can find $b_i \in \{0, 1, -1\}$ such that
$$N = b_0 + 2b_1 + \cdots + 2^{k+1} b_{k+1}$$
and such that among two successive b_i at least one of them is equal to zero. Describe an algorithm that computes such b_i from the a_i.
5. Describe an algorithm to compute NP from an expression of N of the form given in the previous question, and compute exactly the number of operations that it requires, in terms of the number of zeroes and ± 1 among the b_i. What is this number in the worst case ?

6. *This question is independent of the previous ones.* We consider the following key exchange protocol between Alice and Bob : They choose a public elliptic curve E on $\mathbb{Z}/p\mathbb{Z}$ and a point $P \in E(\mathbb{Z}/p\mathbb{Z})$. Alice chooses secretly a number n_A and Bob chooses secretly a number n_B. Alice computes $Q_A = n_A P$ and then sends Q_A to Bob. Bob computes $Q_B = n_B P$ and then sends Q_B to Alice. Then, Alice computes $n_A Q_B$ and Bob computes $n_B Q_A$.

a) Explain why Alice and Bpb have now a common secret S.

b) We now assume that Eve is able to intercept the data that Alice and Bob exchange, which problem does she have to solve in order to compute S ?

c) Explain why she is able to compute S if she can solve the discrete log problem in $E(\mathbb{Z}/p\mathbb{Z})$.

d) Informally describe an algorithm that allows Eve to solve the discrete log problem in $E(\mathbb{Z}/p\mathbb{Z})$ in $\tilde{O}(\sqrt{p})$ operations in $E(\mathbb{Z}/p\mathbb{Z})$. What happens if Alice can use a quantum computer ?

Part 2 : Quantum computing

Exercice 1.

Let us recall the quantum key exchange between Alice and Bob. We condider the following two othonormal bases of $\mathcal{B} = \mathbb{C}^2$:

$$\oplus = \{|0\rangle, |1\rangle\} \qquad \otimes = \left\{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}$$

Alice chooses, uniformly and independently, a sequence of bits $(a_1, a_2, \ldots, a_N)$. Next, she chooses, uniformly and independently, a sequence of bases $(\alpha_1, \ldots, \alpha_N) \in \{\oplus, \otimes\}^N$. She sends to Bob a sequence of particules in the quantum states $|\psi_i\rangle$ depending on the pair (a_i, α_i) according to the rule given in the following table :

	$\oplus$	$\otimes$
0	$\|0\rangle$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$
1	$\|1\rangle$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$

Then, it is Bob's turn to choose a sequence of bases $(\beta_1, \ldots, \beta_N) \in \{\oplus, \otimes\}^N$, and to measure in the base β_i the quantum state number i that he has received. He obtains a sequence of bits $(b_1, \ldots, b_N) \in \{0, 1\}^N$.

In the third step, Alice and Bob publish through a public classical channel the two sequences $(\alpha_1, \ldots, \alpha_N)$ and $(\beta_1, \ldots, \beta_N)$, and derive the set I of indices i such that $\alpha_i =$

β_i. They discard from their sequences $a_1, \ldots, a_N$ and $b_1, \ldots b_N$ the entries of index not belonging to I.

Eve is an eavesdropper who can perform a measure of her choice on every state $|\psi_i\rangle$, before the state is sent to Bob.

We were presented during the lecture an analysis of the situation in the case when Eve measures each $|\psi_i\rangle$ in one of the bases $\oplus$ or $\otimes$ (chosen uniformly and independently). We will consider a different strategy were Eve chooses an angle θ, and performs her measures according to the base $\{|e_0\rangle, |e_1\rangle\}$, where

$$\begin{cases} |e_0\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \\ |e_1\rangle = -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle\,. \end{cases}$$

Said differently, with the notations of the lecture, this measure is the measure associated to the orthogonal projections P_0, P_1 on respectively $|e_0\rangle$ and $|e_1\rangle$.

1. Recall, given a state $|\psi\rangle$, what can be the result of Eve's measure on $|\psi\rangle$ and what happens to this state during the measurement.
2. We assume that $\alpha_i = \beta_i = \oplus$ and that $a_i = 0$. Describe precisely, and with explanations, the state $|\psi_i\rangle$ at the various steps of the protocole : when Alice sends it, after Eve's measurement, after Bob's measurement and give in every case the value of the bit obtained by Eve and by Bob.
3. Same question in the other cases : $\alpha_i = \beta_i = \oplus$ and $a_i = 1$, then $\alpha_i = \beta_i = \otimes$ and $a_i = 0$, $a_i = 1$. In this question, just state the results without too many explanations.
4. Compute the probability that Eve's action can be detected by Alice and Bob during the transmission of one bit of index $i \in I$.
5. Compute the probability that, during the transmission of one bit of index $i \in I$, Eve is not detected, and obtains the correct value of this bit.
6. What is the optimal value of θ for Eve ?
7. In this question, Eve would like to find a way not to be detected. She thinks she can make it if she brings her one particule in state $|e\rangle$ and creates a quantum system in state $|\psi_i\rangle \otimes |e\rangle$. She would like to perform a quantum operation U on this system to that it is transformed to $|\psi_i\rangle \otimes |\psi_i\rangle$, with the goal to measure her qubit (i.e. the second) without modifying Alice's qubit. Show that such an operation, valid for all i, cannot exist.

Part 3 : Euclidean lattices

Exercice 2. We have seen in TD4 that the continued fractions expansion of a real number α allows to compute rational approximations of α verifying $|\alpha - p/q| < 1/(2q^2)$.

Here we consider *simultaneous approximations* of n numbers $\alpha_1, \ldots, \alpha_n$. Dirichlet showed that there are infinitely many integers p_i and q such that $|\alpha_i - p_i/q| < q^{-(1+1/n)}$ for all $i = 1, \ldots, n$. We will see that the LLL algorithm allows to compute such approximations, up to a multiplicative factor that depends only on n.

We assume that individual rational approximations of each α_i are known and we denote them $\beta_i = u_i/v_i$ with $u_i, v_i \in \mathbb{Z}$. We fix an upper bound Q for the denominator q of the desired simultaneous approximations, we set $\epsilon = Q^{-1/n}$ and we choose Q large enough so that $\epsilon < 1$.

Let $w = 2^{-n(n+1)/4}\epsilon^{n+1}$ and let L be the lattice of dimension $n+1$ generated by the columns of the following matrix P :

$$P = \begin{pmatrix} w & 0 & \ldots & 0 \\ \beta_1 & -1 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ \beta_n & 0 & \ldots & -1 \end{pmatrix}$$

We recall that the LLL algorithm computes a base of L whose first vector b_1 satisfies :

$$\|b_1\| \leq 2^{\frac{n}{4}} \det(L)^{\frac{1}{n+1}}.$$

1. Compute $\det(L)$.
2. Show that the LLL algorithm outputs integers $q > 0$ and $p_1, \ldots, p_n$ such that
$$q^2w^2 + (q\beta_1 - p_1)^2 + \cdots + (q\beta_n - p_n)^2 \leq \epsilon^2$$
3. Show that $q \leq 2^{n(n+1)/4}Q$ and that $|\beta_i - p_i/q| < 2^{(n+1)/4}q^{-(1+1/n)}$.
4. What can you say about the complexity of this method ?

Exercice 3. *Ne pas hésiter à faire des dessins..*

The goal of this exercise is to show the following theorem which is due to Hermite :

Théorème : Let L be a lattice of dimension n, there exists a base $\{e_1, \ldots, e_n\}$ of L such that

$$\|e_1\| \ldots \|e_n\| \leq \left(\frac{4}{3}\right)^{\frac{n(n-1)}{4}} \det(L).$$

In what follows, e_1 is a minimal vector of L and $H = (\mathbb{R}e_1)^\perp$ is the hyperplane orthogonal to e_1. Let P denote the orthogonal projection on H, and let $L' = P(L)$ be the projection of the lattice L on H.

1. Show that for all $x' \in L'$, there is $x \in L$ such that $P(x) = x'$ and $\|x\| \leq \sqrt{4/3}\|x'\|$.

2. Let $\{e'_2, \ldots . e'_n\}$ be a base of the lattice L'. Let $e_2, \ldots, e_n$ be elements of L such that $P(e_i) = e'_i$. Show that $\{e_1, e_2, \ldots, e_n\}$ is a base of L.

3. Show that $\det(L) = \|e_1\| \det(L')$.

4. Prove Hermite's theorem by induction on n, with the help of previous questions.

5. Show that Hermite's inequality is optimal in dimension 2. Compare, for arbitrary n, with the analogous inequality satisfied by an LLL reduced basis.