Année universitaire 2018-2019, session 1

UE 4TMA901EX

Algorithmique et arithmétique

Master mention *Mathématiques et applications*

Enseignants responsables : Christine Bachoc et Jean-Marc Couveignes.

Examen du jeudi 13/12/2018 à 9h (durée trois heures)

$\star\star\star$

Calculette autorisée. Documents non-autorisés.

$\star\star\star$

La notation accordera la plus grande importance à la qualité de la rédaction.

Part I.

Exercise 1 :

We want to factor the integer $N = 20737$ using the quadratic sieve.

1 . We notice that $\sqrt{N} \simeq 144.0035$. We set $m = 144$. Write a congruence modulo N of the type

$$(a+m)^2 \equiv a^2 + u_1 a + u_0 \bmod N$$

depending on an integer parameter a. Here u_0, u_1 are well chosen integer constants.

2 . Find values of a in the interval $[-20, 20]$ that produce a congruence between a square and a smooth number (in a sense to be made precise) modulo N. You may use the following data.

```
? for(a=-20,20,print([a,factor(a^2+a*288-1)]))
[-20, [-1, 1; 3, 1; 1787, 1]]
[-19, [-1, 1; 2, 3; 3, 2; 71, 1]]
[-18, [-1, 1; 4861, 1]]
[-17, [-1, 1; 2, 9; 3, 2]]
[-16, [-1, 1; 3, 1; 1451, 1]]
[-15, [-1, 1; 2, 12]]
[-14, [-1, 1; 3, 1; 1279, 1]]
[-13, [-1, 1; 2, 3; 3, 1; 149, 1]]
[-12, [-1, 1; 3313, 1]]
[-11, [-1, 1; 2, 3; 3, 1; 127, 1]]
[-10, [-1, 1; 3, 3; 103, 1]]
[-9, [-1, 1; 2, 4; 157, 1]]
```

```
  [-8, [-1, 1; 3, 3; 83, 1]]
* [-7, [-1, 1; 2, 4; 3, 1; 41, 1]]
  [-6, [-1, 1; 1693, 1]]
  [-5, [-1, 1; 2, 3; 3, 1; 59, 1]]
  [-4, [-1, 1; 3, 1; 379, 1]]
  [-3, [-1, 1; 2, 3; 107, 1]]
  [-2, [-1, 1; 3, 1; 191, 1]]
* [-1, [-1, 1; 2, 5; 3, 2]]
  [0, Mat([-1, 1])]
* [1, [2, 5; 3, 2]]
  [2, [3, 1; 193, 1]]
  [3, [2, 3; 109, 1]]
  [4, [3, 1; 389, 1]]
  [5, [2, 3; 3, 1; 61, 1]]
* [6, [41, 1; 43, 1]]
* [7, [2, 4; 3, 1; 43, 1]]
  [8, [3, 2; 263, 1]]
  [9, [2, 4; 167, 1]]
  [10, [3, 2; 331, 1]]
  [11, [2, 3; 3, 1; 137, 1]]
  [12, [59, 1; 61, 1]]
  [13, [2, 3; 3, 1; 163, 1]]
  [14, [3, 1; 1409, 1]]
  [15, [2, 6; 71, 1]]
  [16, [3, 1; 1621, 1]]
* [17, [2, 6; 3, 4]]
  [18, Mat([5507, 1])]
* [19, [2, 3; 3, 6]]
  [20, [3, 1; 2053, 1]]
```

3 . Write down all the congruences you have found. Report the signs and valuations in a matrix M with integer coefficients.

4 . Compute (a basis of) the kernel of the reduction modulo 2 of the matrix M.

5 . For each vector in this basis write a congruence between two squares modulo N. Deduce a factorization of N.

Exercise 2 :

Let G be the group $\mathbb{F}_7^*$.

1 . Give a generator g of G.

2 . Give the table of the discrete exponential function with basis g

$$\exp_g : x \mapsto g^x.$$

3 . Give the table of the discrete logarithm function with basis g

$$\log_g : h \mapsto x \text{ such that } h = g^x.$$

4 . Compute $g^{10^{100}+10^{10}+1}$.

Exercise 3 :

Let $\mathbf{K}$ be the field $\mathbb{Z}/5\mathbb{Z}$. Let C be the affine curve with equation

$$y^2 = x^3 + x + 2$$

over $\mathbf{K}$.

1 . Prove that C is smooth.

2 . Compute all the points on C with coordinates in $\mathbf{K}$.

Let $C \cup \{O\}$ be the elliptic curve obtained by adding the point O at infinity to the affine curve C.

3 . Recall the definition of the group law on $C(\mathbf{K}) \cup \{O\}$. What is the order of this group ?

4 . Let Q be the point with coordinates $x_Q = 1$ et $y_Q = 2$. Compute $[321234567898765432123]Q$.

Université de Bordeaux
Master Mathématiques et Applications
Année 2018-2019

Algorithmique Arithmétique

13 décembre 2018

Documents are not allowed
The exercises are independent

Exercise 1 : Quantum computing

We consider the following *parity game* with two players Alice and Bob. Two bits x and y, chosen uniformly and independently in $\{0,1\}$, are given respectively to Alice and Bob. Alice does not know Bob's bit y, and conversely Bob does not know Alice's bit x. Then, each of them is asked to produce one bit, respectively a for Alice and b for Bob, and they win the game if $a + b = xy \bmod 2$.

Alice and Bob can discuss before the game starts and decide for a strategy, but they cannot communicate during the game.

1. Alice and Bob decide that they will play $a = 0$ and $b = 0$, whatever the values of their bits. Compute their probability of winning the game.
2. Show that this probability cannot be improved with another strategy (hint : a and b can be modelled by boolean functions $a(x)$, $b(y)$ from $\{0,1\}$ to $\{0,1\}$. There are four such boolean functions : $x \mapsto 0, 1, x, 1+x$. Compute $a(x) + b(y) + xy \bmod 2$ in each case.

Now, Alice and Bob are given some quantum power, and we will see that it will improve their chances of winning the game. More precisely, they share a system of two particules whose quantum state is $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice can perform quantum operations and measurements on her particule, which means that she can act on the first qubit, and Bob can act on the second qubit. They decide that they will apply the following strategy *in this order* during the game :

— If $x = 0$, Alice doesn't do anything, but if $x = 1$ she applies the rotation of angle $\pi/8$ to her qubit.

— If $y = 0$, Bob doesn't do anything, but if $y = 1$ he applies the rotation of angle $-\pi/8$ to his qubit.

— Alice measures her qubit and outputs a, the result of her measurement.

— Bob measures his qubit and outputs b, the result of his measurement.

3. If $x = y = 0$, show that the probability that $a = b$ is equal to 1.
4. If $x \neq y$, show that the probability that $a = b$ is equal to $\cos^2(\pi/8)$.
5. If $x = y = 1$, show that the probability that $a \neq b$ is equal to $1/2$.
6. From the previous questions, deduce that the winning probability of Alice and Bob is equal to $(4\cos^2(\pi/8) + 3)/8 \approx 0.80$.

We recall that the matrix of a rotation of angle θ is $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. *Also, it may be useful to remember and apply the following trigonometric formulas :*
$\cos^2\theta + \sin^2\theta = 1$, $\cos 2\theta = \cos^2\theta - \sin^2\theta$, $\sin 2\theta = 2\cos\theta\sin\theta$.

Exercise 2 : Euclidean lattices

We follow the notations introduced during the lecture. Let $\{b_1, \ldots, b_n\}$ be a basis of $\mathbb{R}^n$. Its Gram-Schmidt orthogonalisation is the basis $\{b'_1, \ldots, b'_n\}$ such that $\langle b'_i, b'_j \rangle = 0$ for $i \neq j$, $1 \leq i, j \leq n$, and such that there are numbers $u_{i,j}$ with $b_i = b'_i + \sum_{j=1}^{i-1} u_{i,j} b'_j$. We recall that a basis $\{b_1, \ldots, b_n\}$ is said to be LLL reduced if it satisfies the two conditions :

— *For all $1 \leq j < i \leq n$, $-1/2 \leq u_{i,j} \leq 1/2$*

— *For all $2 \leq i \leq n$, $\|b'_i\|^2 \geq (3/4 - u_{i,i-1}^2)\|b'_{i-1}\|^2$*

Let $L \subset \mathbb{R}^n$ be a lattice and let $\{b_1, \ldots, b_n\}$ be a basis of L.

1. Show that $\det(L) = \prod_{i=1}^n \|b'_i\|$.

Now we assume that $\{b_1, \ldots, b_n\}$ is LLL reduced.

2. Show that, for all $1 \leq j < i$, $\|b'_j\|^2 \leq 2^{i-j}\|b'_i\|^2$.
3. Applying 2., show that $\|b_1\| \leq 2^{(n-1)/4}(\det(L))^{1/n}$ and hence that
$$\min(L) \leq 2^{(n-1)/4}\det(L)^{1/n}.$$
4. Deduce from 2. that, for all $1 \leq i \leq n$, $\|b_i\|^2 \leq 2^{i-1}\|b'_i\|^2$ and hence that
$$\prod_{i=1}^n \|b_i\| \leq 2^{n(n-1)/4}\det(L).$$