Année universitaire 2020-2021, session 1

UE 4TMA901EX

Algorithmique arithmétique

Master mention *Mathématiques et applications*

Enseignants responsables : Xavier Caruso et Jean-Marc Couveignes.

Examen du jeudi 10/12/2020 à 14h30 (durée trois heures)

⋆⋆⋆

Calculette autorisée. Documents non-autorisés.
Calculators are allowed. Documents are not.

⋆⋆⋆

Ce sujet comporte deux parties à rédiger sur deux copies différentes.
This examination consists of two parts. Please write on two distinct papers.

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

Part I.

Exercise 1 :

We want to factor the integer $N = 36103$ with the quadratic sieve.

1. We compute $\sqrt{N} \simeq 190.007894$. Write a congruence modulo N of the form

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

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

2. Look for values of a in the interval $[-20, 20]$ that produce a congruence between a square and a 7-smooth integer. You may use the data below.

```
for(a=-20,20,print([a,factor(a^2+380*a-3)]))
[-20, [-1, 1; 3, 1; 7, 4]]
[-19, [-1, 1; 2, 1; 47, 1; 73, 1]]
[-18, [-1, 1; 3, 1; 41, 1; 53, 1]]
[-17, [-1, 1; 2, 1; 3, 2; 7, 3]]
[-16, [-1, 1; 5827, 1]]
[-15, [-1, 1; 2, 1; 3, 1; 11, 1; 83, 1]]
[-14, [-1, 1; 3, 1; 1709, 1]]
[-13, [-1, 1; 2, 1; 7, 1; 11, 1; 31, 1]]
```

```
[-12, [-1, 1; 3, 2; 491, 1]]
[-11, [-1, 1; 2, 1; 3, 1; 677, 1]]
[-10, [-1, 1; 7, 1; 23, 2]]
[-9, [-1, 1; 2, 1; 3, 1; 557, 1]]
[-8, [-1, 1; 3, 2; 331, 1]]
[-7, [-1, 1; 2, 1; 1307, 1]]
[-6, [-1, 1; 3, 1; 7, 1; 107, 1]]
[-5, [-1, 1; 2, 1; 3, 1; 313, 1]]
[-4, [-1, 1; 11, 1; 137, 1]]
[-3, [-1, 1; 2, 1; 3, 4; 7, 1]]
[-2, [-1, 1; 3, 1; 11, 1; 23, 1]]
[-1, [-1, 1; 2, 1; 191, 1]]
[0, [-1, 1; 3, 1]]
[1, [2, 1; 3, 3; 7, 1]]
[2, Mat([761, 1])]
[3, [2, 1; 3, 1; 191, 1]]
[4, [3, 1; 7, 1; 73, 1]]
[5, [2, 1; 31, 2]]
[6, [3, 2; 257, 1]]
[7, [2, 1; 3, 1; 11, 1; 41, 1]]
[8, [7, 1; 443, 1]]
[9, [2, 1; 3, 1; 11, 1; 53, 1]]
[10, [3, 2; 433, 1]]
[11, [2, 1; 7, 1; 307, 1]]
[12, [3, 1; 1567, 1]]
[13, [2, 1; 3, 1; 23, 1; 37, 1]]
[14, [37, 1; 149, 1]]
[15, [2, 1; 3, 2; 7, 1; 47, 1]]
[16, [3, 1; 2111, 1]]
[17, [2, 1; 3373, 1]]
[18, [3, 1; 7, 1; 11, 1; 31, 1]]
[19, [2, 1; 3, 2; 421, 1]]
[20, [11, 1; 727, 1]]
```

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

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

5. From every element in this basis deduce a congruence between two squares modulo N. Deduce a (possibly trivial) factorization of N.

Exercise 2 :

1. Give the list of all irreducible polynomials with degree $\leqslant 2$ in $\mathbb{F}_2[x]$.

2. Le $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Prove that $f(x)$ is irreducible.

3. Let $\mathbb{K} = \mathbb{F}_2[x]/f(x)$. Prove that $\mathbb{K}$ is a field.

4. Let $a = x \bmod f(x)$. Compute a^3 and a^5. Prove that a is a generator of $\mathbb{K}$.

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 $\mathbf{K}$.

3. Let E be the projective (elliptic) curve with homogeneous equation

$$Y^2Z = X^3 - XZ^2 + 2Z^3.$$

Let $P \in E(\mathbf{K})$ be the point with coordinates $(3:1:1)$. Let $O = (0:1:0)$. Prove that

$$[3]P = P \oplus P \oplus P = O.$$

Compute $[10000000001]P$.

Part II.

Exercise 1 (Emulating the controlled phase shift gate):

We recall the definition of the following gates:

- the X-gate acts on 1-qubits by $|0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto |0\rangle$
- the CX-gate acts on 2-qubits by $|00\rangle \mapsto |00\rangle$, $|01\rangle \mapsto |01\rangle$, $|10\rangle \mapsto |11\rangle$ and $|11\rangle \mapsto |10\rangle$
- for $\theta \in \mathbb{R}$, the phase shift gate R_θ acts on 1-qubits by $|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto e^{i\theta}|1\rangle$
- for $\theta \in \mathbb{R}$, the controlled phase shift gate CR_θ acts on 2-qubits by $|00\rangle \mapsto |00\rangle$, $|01\rangle \mapsto |01\rangle$, $|10\rangle \mapsto |10\rangle$, $|11\rangle \mapsto e^{i\theta}|11\rangle$.

We say that a circuit is *reduced* if it is only made of X-gates, CX-gates and phase shift gates. We set $q_0 = |00\rangle$, $q_1 = |01\rangle$, $q_2 = |10\rangle$ and $q_3 = |11\rangle$.

1. For each subset $I \subset \{0, 1, 2, 3\}$ of cardinality 2, write a reduced circuit that acts on 2-qubits by $q_i \mapsto e^{i\theta} q_i$ for $i \in I$ and $q_i \mapsto q_i$ for $i \notin I$.

2. Write a reduced circuit that emulates the gate CR_θ.

Exercise 2 (EPR triple):

We consider the following SageMath code:

```
QC = QuantumComputer()
a = QC.malloc(1)
b = QC.malloc(1)
c = QC.malloc(1)
QC.hadamard(a)
QC.hadamard(b)
QC.CCX(a, b, c)      # a and b are the controlling bits
if QC.measure(c) == 1:
    raise RuntimeError
QC.CX(a, c)          # a is the controlling bit
QC.CX(b, c)          # b is the controlling bit
QC.X(c)
```

1. What is the probability that the above code raises a `RuntimeError`?

2. When no error occurs, what is the internal state of the quantum computer `QC` after the execution of the above code?

3. Is it possible to obtain the same internal state by only applying X-gates, CX-gates, CCX-gates and Hadamard gates (but no measures)?

Exercise 3:

Let p be an odd prime number.

1. Solve the equation $x^2 \equiv 1 \pmod{p}$.

2. By induction on n, solve the equation $x^2 \equiv 1 \pmod{p^n}$.

3. Show that Shor's factorization algorithm always fails if the input integer (that is the number we want to factor) is a power of an odd prime number. What could we do to fix this issue?