UE 4TMA901EX
Algorithmique Arithmétique

Contrôle du 19/12/2019, de 14h30 à 17h30

⋆⋆⋆

Calculette et documents autorisés.
Calculators and documents are allowed.

⋆⋆⋆

Ce sujet comporte deux parties à rédiger sur deux copies différentes.
Please treat part I and part II on two different papers.

Part I

Exercice 1:
Solve the equation $a^2 = 308 \bmod 437$.
Detail and justify each step.

Exercice 2:
Solve the equation $a^{67} = 54 \bmod 101$.

Exercice 3:
Check that $f(x) = x^3 + x^2 - x + 1 \in \mathbb{F}_3[x]$ is irreducible. Let $\mathbf{K} = \mathbb{F}_3[x]/f(x)$.
Solve the equation $a^9 = x \bmod f(x)$.

Exercice 4:
Prove that 3 is a generator of $(\mathbb{Z}/31\mathbb{Z})^*$.

Exercice 5:
We want to factor $N = 6401$ using the quadratic sieve.

1 . We note that $\sqrt{N} \simeq 80.0062$. Write a congruence modulo N like

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

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

2 . The following code

```
for(a=-40,40,print([a,factor(a^2+160*a-1)]))
```

produces (among others)

```
[-31, [-1, 1; 2, 5; 5, 3]]
[-29, [-1, 1; 2, 3; 5, 2; 19, 1]]
[-17, [-1, 1; 2, 7; 19, 1]]
[-15, [-1, 1; 2, 7; 17, 1]]
[-9, [-1, 1; 2, 4; 5, 1; 17, 1]]
[-4, [-1, 1; 5, 4]]
[-1, [-1, 1; 2, 5; 5, 1]]
[0, Mat([-1, 1])]
[1, [2, 5; 5, 1]]
[2, [17, 1; 19, 1]]
[9, [2, 4; 5, 1; 19, 1]]
[19, [2, 3; 5, 2; 17, 1]]
[21, [2, 3; 5, 2; 19, 1]]
[25, [2, 4; 17, 2]]
```

Write down the interesting congruences that you can deduce from this calculation. Report the signs and valuations in a matrix M with integer coefficients.

3 . Compute the kernel of M modulo 2. Give a basis of it.

4 . For any vector in this basis write down a congruence between two squares modulo N. Deduce a (preferably non trivial) factorization of N.

Exercice 6:
Let E be the projective curve with equation $Y^2Z = X^3 + XZ^2 + Z^3$ over the field $\mathbb{F}_7$ with 7 elements.

1 . Prove that E is a smooth curve.

2 . Write the list of all points on E with coordinates in $\mathbb{F}_7$.
What is the group structure of $E(\mathbb{F}_7)$?

3 . Let $P = (2 : 5 : 1)$. Give the equation of the tangent to E at P. Compute $P \oplus P$.

Part II

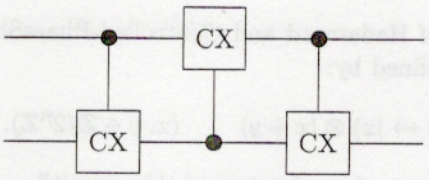
Exercice 1 (On the impossibility to duplicate a qubit):

We denote by $Q_1 = \mathbb{C}\,|0\rangle \oplus \mathbb{C}\,|1\rangle$ the $\mathbb{C}$-vector space of (unnormalized) 1-qubits.
We denote by $Q_2 = \mathbb{C}\,|00\rangle \oplus \mathbb{C}\,|01\rangle \oplus \mathbb{C}\,|10\rangle \oplus \mathbb{C}\,|11\rangle$ the $\mathbb{C}$-vector space of (unnormalized) 2-qubits.

Prove that there is *no* unitary transformation $f : Q_1 \to Q_2$ such that $f(q) = q \otimes q$ for all $q \in Q_1$.

Exercice 2 (The Controlled-SWAP gate):

1 . Compute the action of the following circuit on each pure 2-qubit ($|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$).



(We recall that CX denotes the Controlled-NOT gate; it acts on a 2-qubit as follows: when the controlling bit is 0, it leaves the input unchanged, when it is 1, it flips the other bit.)

2 . The Controlled-SWAP gate is the gate acting on a 3-qubit as follows:

$$|0xy\rangle \mapsto |0xy\rangle$$
$$|1xy\rangle \mapsto |1yx\rangle$$

for $x, y \in \{0, 1\}$.

a) Write a circuit only made of Toffoli gates which realizes the Controlled-SWAP gate.

b) Write a circuit only made of Controlled-NOT gates and *one* Toffoli gate which realizes the Controlled-SWAP gate.

Exercice 3 (Inplace additioner *via* Quantum Fourier Transform):

Throughout this exercise, n is a fixed positive integer.
We recall that the Fourier transform of a function $f : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{C}$ is the function $\hat{f} : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{C}$ defined by:

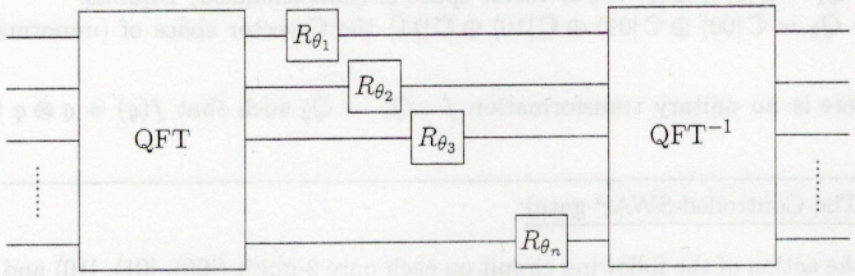
$$\hat{f}(y) = \frac{1}{2^{n/2}} \cdot \sum_{x=0}^{2^n-1} \exp\left(\frac{2i\pi xy}{2^n}\right) f(x).$$

1 . Compute the Fourier transform of a constant function.

2 . Let $f : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{C}$ be any function and $a \in \mathbb{Z}/2^n\mathbb{Z}$. Let $g : \mathbb{Z}/2^n\mathbb{Z} \to \mathbb{C}$ be the function defined by $g(x) = f(x + a)$. Prove that:

$$\hat{g}(y) = \exp\left(-\frac{2i\pi ay}{2^n}\right) \cdot \hat{f}(y).$$

3 . We write QFT (resp QFT^{-1}) for a quantum gate acting on a n-qubit and realizing on it the Fourier transform (resp. the inverse Fourier transform) modulo 2^n.
For $\theta \in \mathbb{R}$, we denote by R_θ the Phase Shift gate acting on a 1-qubit by $|0\rangle \mapsto |0\rangle$, $|1\rangle \mapsto e^{i\theta}|1\rangle$.
Let $a \in \mathbb{Z}/2^n\mathbb{Z}$. Determine angles $\theta_1, \ldots, \theta_n$ for which the following circuit realizes the addition by a (*i.e.* acts as $|x\rangle \mapsto |(x+a)\rangle$ for $x \in \mathbb{Z}/2^n\mathbb{Z}$).



4 . Write a circuit made only of Hadamard and Controlled-PhaseShift gates which realizes the addition gate modulo 2^n, defined by:

$$|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |x+y\rangle \qquad (x, y \in \mathbb{Z}/2^n\mathbb{Z}).$$

What is the complexity (*i.e.* the number of gates) of this circuit?