Exercice 2

(a) Because $U$ is a unitary with eigenvalues in $\{-1, 1\}$, we can write $U = P_0 - P_1$. Let $V = P_0 + iP_1$. We have

$$V^2 = (P_0 + iP_1)^2 = P_0^2 + iP_0P_1 + iP_1P_0 + i^2P_1^2 = P_0^2 - P_1^2 = P_0 - P_1$$

(b) Apply a Hadamard on the first qubit, a controlled-$U$, and and a Hadamard on the first qubit. If $U(|\psi\rangle) = |\psi\rangle$, we get

$$|0\rangle|\psi\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle + |1\rangle|\psi\rangle) \rightarrow \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle + |1\rangle|\psi\rangle) \rightarrow |0\rangle|\psi\rangle.$$  

If $U(|\psi\rangle) = -|\psi\rangle$, we get

$$|0\rangle|\psi\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle + |1\rangle|\psi\rangle) \rightarrow \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle - |1\rangle|\psi\rangle) \rightarrow |1\rangle|\psi\rangle.$$  

(c) Let $W$ be the unitary of question (b). We want to construct the unitary $V$. Since, $V = P_0 + iP_1$, we have : if $U(|\psi\rangle) = |\psi\rangle$ then $V(|\psi\rangle) = |\psi\rangle$; if $U(|\psi\rangle) = -|\psi\rangle$ then $V(|\psi\rangle) = i|\psi\rangle$. In order to construct $V$ (with an additional ancillary qubit on the left), we apply $W$, $Z_i$ on the first qubits and $W^\dagger$ where $Z_i(|b\rangle) = i|b\rangle$.

\[
\begin{array}{l}
\text{if } U(|\psi\rangle) = |\psi\rangle \rightarrow |0\rangle|\psi\rangle \xrightarrow{W} |0\rangle|\psi\rangle \xrightarrow{Z_i \otimes I} |0\rangle|\psi\rangle \xrightarrow{W^\dagger} |0\rangle|\psi\rangle \\
\text{if } U(|\psi\rangle) = -|\psi\rangle \rightarrow |0\rangle|\psi\rangle \xrightarrow{W} |1\rangle|\psi\rangle \xrightarrow{Z_i \otimes I} -i|1\rangle|\psi\rangle \xrightarrow{W^\dagger} i|0\rangle|\psi\rangle \\
\end{array}
\]

the above exactly constructs $V$ with an extra ancilla qubit on the left.

Exercice 3

(a) $|\psi_1\rangle = \frac{1}{p}\sum_{x,y \in \mathbb{F}_p} |x\rangle|y\rangle|0\rangle$.  


– (b) \( |\psi_2\rangle = \frac{1}{p} \sum_{x,y \in \mathbb{F}_p} |x\rangle |y\rangle f(x,y) \). For any \( \gamma \), \( f(x,y) \) is constant on the curve \( P_\gamma \): \( \{(x,y) : mx - y = \gamma\} \) and \( f(x,y) \neq f(x',y') \) if they are not on the same curve. Each curve has the same number of points so each outcome is uniform. This means that after measuring the third register, the state collapses to

\[
|\psi_3\rangle = \frac{1}{\sqrt{p}} \sum_{x,y : f(x,y) = u} |x\rangle |y\rangle.
\]

where \( u \) is the measured outcome. We can rewrite \( |\psi_3\rangle \) as \( \frac{1}{\sqrt{p}} \sum_{x,y \in P_\gamma} |x\rangle |y\rangle = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} |x\rangle |mx - \gamma\rangle \), for an unknown value \( \gamma \). We use here that for any \( x, \gamma \), there is a unique \( y \) such that \( (x,y) \in P_\gamma \).

– (c) we apply \( QFT_1^\dagger \) once on register 1 and once on register 2. We get the state

\[
ket\psi_4 = \frac{1}{p^{1/2}} \sum_{u,v \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_p} \omega^{-ux-v(mx-\gamma)} |u\rangle |v\rangle
\]

\[
= \omega^{u\gamma} \frac{1}{p^{1/2}} \sum_{u,v \in \mathbb{F}_p} \left( \sum_{x \in \mathbb{F}_p} \omega^{x(-u-vm)} \right) |u\rangle |v\rangle
\]

We use that \( \sum_x \omega^{xA} = 0 \) when \( A \neq 0 \) and \( \sum_x \omega^{xA} = p \) when \( A = 0 \). This shows that when we measure \( u,v \), we only get outcomes such that \( -u - vm = 0 \). If \( v \neq 0 \), we can obtain \( m = \frac{-u}{v} \).