Exercise 8

Part 1

We have to prove that the classically controlled Cu is not Clifford ($CuP_jCu^\dagger \notin P_j$).

When measuring in the Z basis, like we are doing here, there are two possible outocomes: Either 0 or 1.

When measuring the qubit, we apply a projector. In case of the Z measurement, where we get 1 as a result, we apply the the projector $\mathbb{P}_1 = |1\rangle\langle 1|$ and normalize the state. Therefore the post-measurement state $|\psi'\rangle = \frac{\mathbb{P}_1|\psi\rangle}{\sqrt{p_1(|\psi\rangle)}} = |1\rangle$. If we get a 0, the post-measurement state is $|\psi'\rangle = \frac{\mathbb{P}_0|\psi\rangle}{\sqrt{p_0(|\psi\rangle)}} = |1\rangle$

When the outcome of the measurement is 0, because we don't apply the Unitary U, the final state becomes $|0\rangle \otimes \frac{1}{\sqrt{N_0}} \sum_x c_{0x}|x\rangle$, where $N_0 = 1 - \sum_x (c_{1x})^2 = \sum_x |c_{0x}|^2$

Therefore in total when the measurement results in $|0\rangle$, we apply the operator $\mathbb{P}_0 \otimes I = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$. We can show that this operator is Clifford (n is the number of qubits, without the control qubit and $p \in P_n$):

$$
\begin{aligned}
(\mathbb{P}_0 \otimes I_n) \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} (\mathbb{P}_0 \otimes I)^\dagger &= \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix} \\
&= \begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix} \\
&= \begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix} \notin P_{n+1}
\end{aligned}
$$

This part of the operator is not clifford.

When the outcome of the measurement is 1, because we apply the unitary, the final state after the classically controlled unitary is $|1\rangle \otimes \frac{1}{\sqrt{N_1}} \sum_x c_{1x} U|x\rangle$, where $N_1 = 1 - \sum_x (c_{0x})^2 = \sum_x |c_{1x}|^2$.
Therefore in total, if the measurement results in $|1\rangle$, we apply the operator $\mathbb{P}_1 \otimes U$. We can show that this is not Clifford (n is the number of qubits that U acts on, and $p \in P_n$):

$$
\begin{aligned}
(\mathbb{P}_1 \otimes U) \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} (\mathbb{P}_1 \otimes U)^\dagger &= \begin{pmatrix} 0 & 0 \\ 0 & U \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & U^\dagger \end{pmatrix} \\
&= \begin{pmatrix} 0 & 0 \\ 0 & UpU^\dagger \end{pmatrix} \notin P_{n+1}
\end{aligned}
$$

Thus this part of the controlled unitary is not Clifford either.
In total, the controlled unitary can be expressed as

$$
CU = \mathbb{P}_0 \otimes I + \mathbb{P}_1 \otimes U = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}
$$

CU is unitary, because U is Clifford and therefore

$$
\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & U^\dagger \end{pmatrix} = \begin{pmatrix} II & 0 \\ 0 & UU^\dagger \end{pmatrix} = I
$$

To prove that CU is not Clifford, we show that (n is the number of qubits U acts on and $p \in P_n$)

$$\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & U^\dagger \end{pmatrix} = \begin{pmatrix} p & 0 \\ 0 & Up \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & U^\dagger \end{pmatrix}$$
$$= \begin{pmatrix} p & 0 \\ 0 & UpU^\dagger \end{pmatrix} \notin P_{n+1}$$

Part 2

To prove that U is unitary, we have to show, that

$$UU^\dagger = I = \sum_{y=0}^{2^L-1} |f(y)\rangle\langle y| \left(\sum_{y=0}^{2^L-1} |f(y)\rangle\langle y| \right)^\dagger$$

Because $f(y) = x \times y \mod N$, where $x < N \leq 2^L - 1$ and $\gcd(x, N) = 1$ for $0 \geq y < N$, and $f(y) = y$ otherwise

$$U = \sum_{y=0}^{N-1} |x \times y \mod N\rangle\langle y| + \sum_{y=N}^{2^L-1} |y\rangle\langle y|$$

For an operator to be unitary, it must map a base to a base. In this case is the same, so we have to prove that every unique input maps to a unique output, or that f is bijective.
For the second part f ($f(y) = y$ when $N \leq y \leq 2^L - 1$) this is obvious.
For the first part ($f(y) = x \times y \mod N$ when $0 \leq y < N$), we do a standard bijection proof:

1. First to prove that a function is bijective, we must prove that the function is injective, means that if ($f(y) = f(x)$, then $y = x$).

$$\begin{aligned} x \times y_1 = x \times y_2 \mod N \\ y_1 = y_2 \mod N \end{aligned}$$

   Because $y_1 < N$ and $y_2 < N$, $y_1 = y_2$ holds and thus f is injective.
2. Finally we have to prove that f is surjective. Here we have to proove that for every $0 \leq p < N$, there is a $0 \leq y < N$, such that $f(y) = x \times y \mod N = p$

$$x \times y(\mod N) = p$$

   Because $p < N$:

$$x \times y = p \mod N$$

   Now it's obvious to see that there is a p such that $p = x \times y$.
   This proves that the operator is unitary. qed.

Part 3

a) It is quite obvious that the state $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |x^k \mod N\rangle$ is an eigenstate of U, because applying U just "shifts" them around (x^k becomes x^{k+1}) which turns them from a superposition of all of the states up to $r-1$ to a superposition up to $r-1$. The phase in front are just inverse of the roots of unity ($\exp\left(\frac{-2\pi isk}{r}\right)$).

We need to solve for the eigenvalues, by solving the following equation:

$$\begin{aligned} U|u_s\rangle = u_s|u_s\rangle =& U\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left(\frac{-2\pi isk}{r}\right)\left|x^k \mod N\right\rangle \\ =&\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left(\frac{-2\pi isk}{r}\right)\left|(x^k \mod N)\times x \mod N\right\rangle \\ =& u_s\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left(\frac{-2\pi isk}{r}\right)\left|x^k \mod N\right\rangle \end{aligned}$$

b) The eigenvalues of the searched eigenstates are 1 if $\exp\left(\frac{2\pi is}{r}\right) = 1$, which is the case when $s = nr \; \forall n \in \mathbb{Z}$.
Thus, the eigenstates with the eigenvalue 1, are

$$|u_n\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left(-2\pi ink\right)\left|x^k \mod N\right\rangle \forall n \in \mathbb{Z}$$