1. $x < N, \quad \gcd(x, N) = 1$

Unitarity means

$$U^\dagger U = \mathbb{1}$$

$$\therefore \sum_{y_1, y_2} |y_1\rangle\langle f(y_1)| f(y_2)\rangle\langle y_2| = \sum_y |y\rangle\langle y|$$

$$\therefore \langle f(y_1) | f(y_2)\rangle = \delta_{y_1, y_2}$$

So every unique input to the function must give a unique output

$$f(y_1) = f(y_2) \text{ iff } y_1 = y_2$$

This is certainly true when $y \geq N$ since $f(y) = y$ in this case.

$f(y)$ for $y \geq N$ will also not share values $f(y)$ for $0 \leq y < N$ due to the $\bmod N$ in the latter

For $0 \leq y_1, y_2 < N$

Let's use the convention $y_1 > y_2$

$f(y_1) - f(y_2) = x(y_1 - y_2) \bmod N$

$\therefore f(y_1) = f(y_2) \Rightarrow x(y_1 - y_2) = nN$

for some integer n

Since x shares no common factors with N, N must be a factor of $y_1 - y_2$.

$\therefore f(y_1) = f(y_2) \Rightarrow y_1 \geq N$

So $f(y_1) = f(y_2)$ is not possible for $0 \leq y_1 < N$

2 a) $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-i2\pi \frac{sk}{r}} |x^k \bmod N\rangle$

$x^r = 1 \bmod N$

$f(x^k \bmod N) = x^{k+1} \bmod N$

$\therefore U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-i2\pi \frac{sk}{r}} |x^{k+1} \bmod N\rangle$

$= \frac{1}{\sqrt{r}} \sum_{k=-1}^{r-2} e^{-i2\pi \frac{s(k-1)}{r}} |x^k \bmod N\rangle$

$\left(\begin{matrix} x^r = 1 \\ \therefore x^{-1} = x^{r-1} \end{matrix}\right) = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-2} e^{-i2\pi \frac{s(k-1)}{r}} |x^k \bmod N\rangle$

$= e^{i2\pi s/r} |u_s\rangle$

b) $f(y) = y \quad N \leq y < 2^L$

So $U|y\rangle = |y\rangle$ for these states