Implement f(x) as Unitary Transformations

- We need to convert f(x) = a^x mod N to a quantum algorithm.

Start with

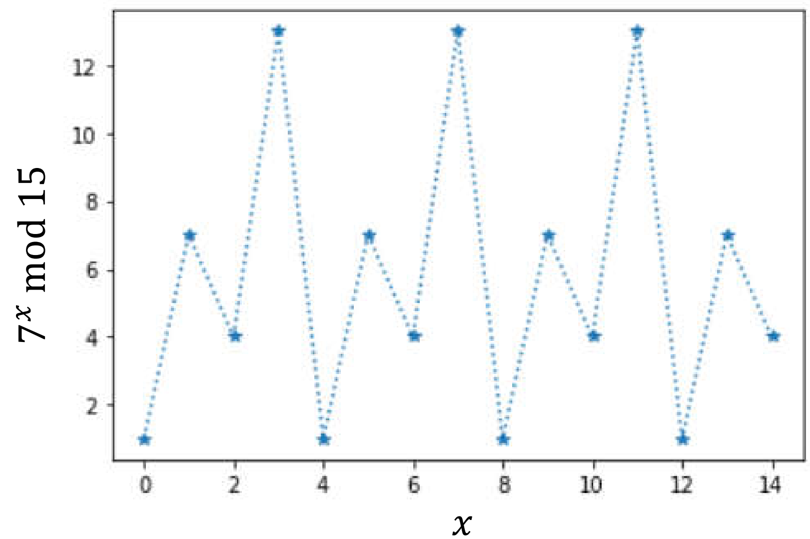
$$\boldsymbol{U}|y\rangle = |ay \bmod 15\rangle$$

and apply multiple times

Consider N = 15 , a = 7

$$\boldsymbol{U}|1\rangle = |1 * 7 \bmod 15\rangle \quad = |7\rangle$$
$$\boldsymbol{U}^2|1\rangle = U(U|1\rangle) = |7 * 7 \bmod 15\rangle = |4\rangle$$
$$\boldsymbol{U}^3|1\rangle = |4 * 7 \bmod 15\rangle \quad = |13\rangle$$
$$\boldsymbol{U}^4|1\rangle = |13 * 7 \bmod 15\rangle \quad = |1\rangle$$

Since the cycle repeats each of these states and any superposition of them is also an eigenstate.



Repeated application with phase

Lets take a well chosen superposition of states (that is also an eigenstate)

$$|u_1\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i k}{r}} \left|a^k \mathrm{mod}\, N\right\rangle$$

This will produce an eigenvalue containing *r*

$$\boldsymbol{U}\,|u_1\rangle = e^{\frac{2\pi i}{r}}|u_1\rangle$$

Moreover there is a family of such solutions with integer *s*

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i\, sk}{r}} \left|a^k \mathrm{mod}\, N\right\rangle$$

$$\boldsymbol{U}|u_s\rangle = e^{\frac{2\pi i\, s}{r}}|u_s\rangle$$

Picking some eigenstates

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i\, sk}{r}} \left|a^k \text{mod } N\right\rangle$$

$|u_s\rangle$ for $0 \le s \le r-1$ are eigenstates with the helpful property that the sum of them all is $|1\rangle$ due to canceling phases

Consider N = 15 , a = 7, r=4

$$\frac{1}{4}(|u_0\rangle + |u_1\rangle + |u_2\rangle + |u_3\rangle)$$

$$\begin{aligned}
= \tfrac{1}{4}(\; & |1\rangle + |7\rangle + |4\rangle + |13\rangle \\
& + |1\rangle + e^{-\frac{2\pi i}{4}} |7\rangle + e^{-\frac{4\pi i}{4}} |4\rangle + e^{-\frac{6\pi i}{4}} |13\rangle \\
& + |1\rangle + e^{-\frac{4\pi i}{4}} |7\rangle + e^{-\frac{8\pi i}{4}} |4\rangle + e^{-\frac{12\pi i}{4}} |13\rangle \\
& + |1\rangle + e^{-\frac{6\pi i}{4}} |7\rangle + e^{-\frac{12\pi i}{4}} |4\rangle + e^{-\frac{18\pi i}{4}} |13\rangle \Big)
\end{aligned}$$

= $|1\rangle$

We knew $|1\rangle$ was an eigenstate, but now we have an, admittedly complex, representation of $|1\rangle$ in $|u_s\rangle$.
Now we know we can use Quantum Phase Estimation on $|1\rangle$ this to find phase $\phi = \frac{s}{r}$.

Doing this in quantum gates

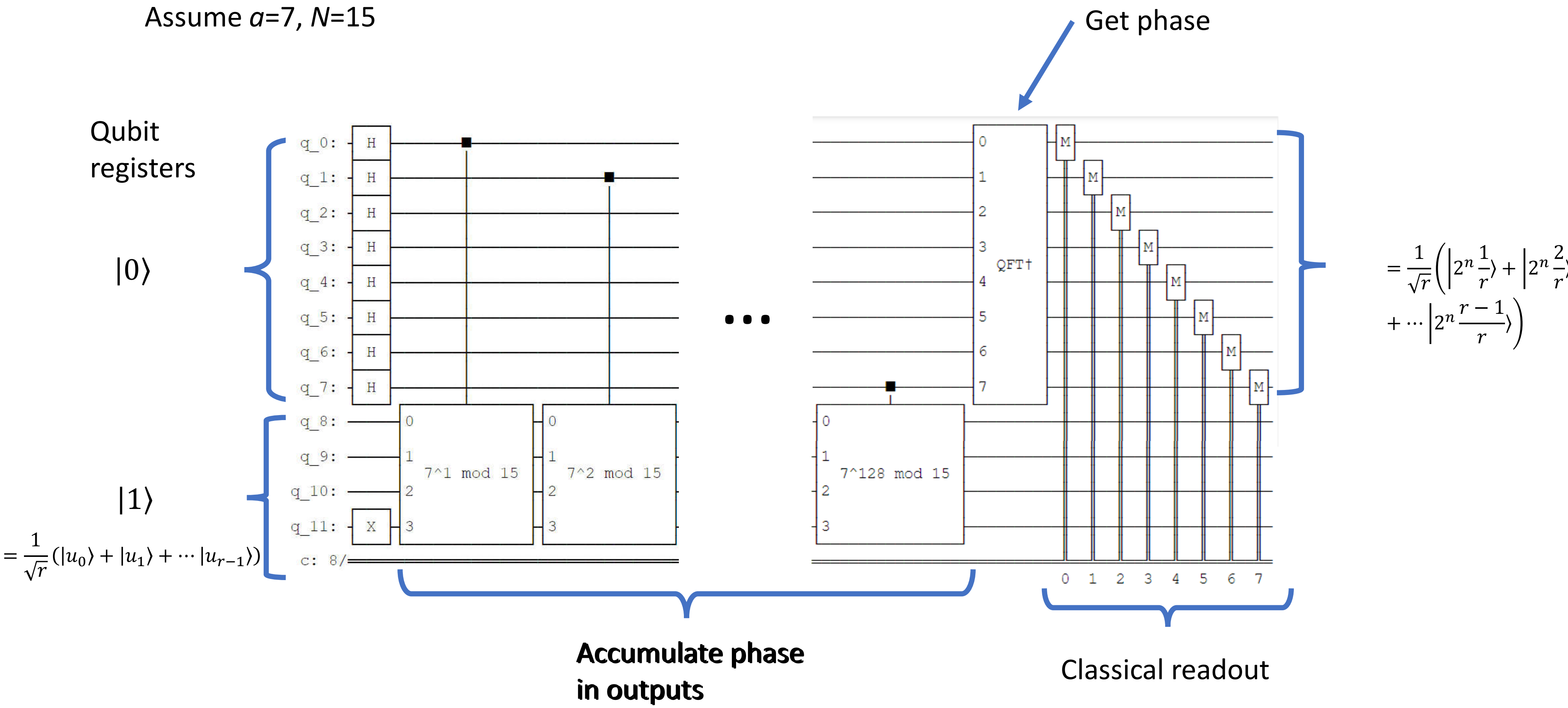
In order to efficiently form **U** for encoded numerical states, we use repeated squaring. Assume we have a form for ***U***, then its easy to show

$$\boldsymbol{U}^{2^j}|y\rangle \;= \underbrace{\boldsymbol{U}^2 \circ \boldsymbol{U}^2 \ldots \circ \boldsymbol{U}^2}_{j\text{ times}}|y\rangle$$

which gives us a polynomial-order for forming $\boldsymbol{U}^{2^j}$

Example Quantum Circuit

Assume *a*=7, *N*=15



Appendix

Proof mod commutes with multiply

Assume m*n mod p with m,n in the form below

mn mod *p with a,b,c,d integers*

*m = a*p+b with b<p (=> b mod p = b)*

*n = c*p+d with d<p*

*mn = (a*p+b)(c*p+d) mod p*

*= acp*p+(ad+bc)*p +bd*

=bd mod p

= bd

*mn = (a*p+b)(c*p+d) mod p*

*= ((a*p+b)mod p)) ((c*p+d) mod p)*

= (b mod p) (d mod p)

= bd