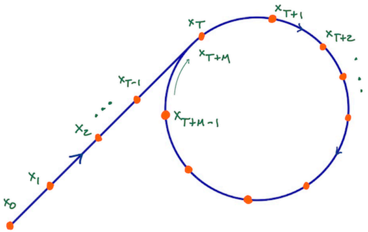
Recall our intuition for Pollard's ρ

Let S be a finite set, $f : S \to S$ a function, and $x_0 \in S$ an initial point



Gives tail of length T and loop of length M

- $T, T+1, T+2, \ldots, T+M-1$ are M consecutive integers
- One must be divisible by M. i.e. One element in loop must look like x_{kM}
- Since the loop has M elements,

$$x_{kM} = x_{KM+M} = x_{KM+2M} = x_{kM+kM} = x_{2kM}$$

- We are guaranteed a collision where $x_i = x_{2i}$ where $i < T + M$!!

Using Pollard's ρ to solve the DLP $g^x \equiv h \mod p$

1. Define $f : \mathbb{F}_p^* \to \mathbb{F}_p^*$:
$$f(x) = \begin{cases} gx & \text{if } 0 \le x < p/3 \\ x^2 & \text{if } p/3 \le x < 2p/3 \\ hx & \text{if } 2p/3 \le x < p \end{cases}$$

2. Define sequence $x_0 = 1$, $x_{i+1} = f(x_i) = g^{\alpha_i} h^{\beta_i}$ where
$$\alpha_{i+1} = \begin{cases} \alpha_i + 1 & \text{if } 0 \le x_i < p/3 \\ 2\alpha_i & \text{if } p/3 \le x_i < 2p/3 \\ \alpha_i & \text{if } 2p/3 \le x_i < p \end{cases} \qquad \beta_{i+1} = \begin{cases} \beta_i & \text{if } 0 \le x_i < p/3 \\ 2\beta_i & \text{if } p/3 \le x_i < 2p/3 \\ \beta_i + 1 & \text{if } 2p/3 \le x_i < p \end{cases}$$

3. Look for collision in sequences $\{x_i\} = \left\{g^{\alpha_i} h^{\beta_i}\right\}$ and $\{y_i\} = \{x_{2i}\} = \left\{g^{\gamma_i} h^{\delta_i}\right\}$

4. This gives $g^u \equiv h^v \mod p$. Take v-th root

1. The purpose of this exercise is to verify that Pollard's ρ will give a collision at $x_i = x_{2i}$

Consider the function $f : \mathbb{Z}/85\mathbb{Z} \to \mathbb{Z}/85\mathbb{Z}$ defined by $f(x) = 5x \mod 85$ and the sequence $\{x_i\}$ formed by $x_0 = 1$, $x_{i+1} = f(x_i)$

(a) What are the first 4 terms in the sequence?

(b) Use the Mathematica notebook to list the first 40 terms of the sequence.

(c) What is T, the length of the tail? What is M, the length of the loop?

(d) What is the value of x_M? Of x_{2M}?

2. Consider applying Pollard's ρ to the DLP $196^x \equiv 787 \mod 1031$

(a) What is the mixing function $f(x)$ in this case?

(b) Fill in the values for the x_1 and y_1 terms in the sequences.
Also verify that the values for x_2 and y_2 are correct.

i	x_i	α_i	β_i	y_i	γ_i	δ_i
0	1	0	0	1	0	0
1						
2	269	2	0	191	4	0

(c) Use the pollardsRho[ ] function defined in the Mathematica notebook to find the collision $x_i = y_i$

(d) Now finish solving the DLP.