Pollard-ρ method:

The goal is to compute x such that

$$g^x = y \quad \text{where}$$

g, y are given, and $y \in \underbrace{\langle g \rangle}_{\text{finite}}$.

$$\langle g \rangle = \{g^0, g^1, g^2, g^3, \dots, g^k, \dots, g^l\}, \quad g^{l+1} = 1 \quad \text{ord } g = l+1$$

$g^0 = 1$

if modulo arithmetic is involved, this is equivalent to $g^2 \pmod p$

We assume that $\text{ord } g = q$ prime number.

For convenience lets assume that $g \in \mathbb{F}_p^*$.

The algorithm will use elements

$$X = g^a y^b \pmod p$$

Let $\langle g \rangle = S_0 \cup S_1 \cup S_2$ such that

$$S_i \cap S_j = \emptyset \quad \text{for } i \neq j$$

Define:

$$f: (X_i, a_i, b_i) \longmapsto (X_{i+1}, a_{i+1}, b_{i+1})$$

in the following way:

$$X_{i+1} = \begin{cases} g \cdot X_i \pmod p & \text{if } X_i \in S_0 \\ X_i^2 \pmod p & \text{if } X_i \in S_1 \\ X_i \cdot y \pmod p & \text{if } X_i \in S_2 \end{cases}$$

$$(a_{i+1}, b_{i+1}) = \begin{cases} (a_i + 1 \bmod q, b_i) & \text{if } X_i \in S_0 \\ (2a_i \pmod q, 2b_i \pmod q) & \text{if } X_i \in S_1 \\ (a_i, b_i + 1 \pmod q) & \text{if } X_i \in S_2 \end{cases}$$

$S_0 := \{X \in \langle g \rangle : X \equiv 1 \pmod 3\}$

$S_1 := \{X \in \langle g \rangle : X \equiv 2 \pmod 3\}$

$S_2 := \{X \in \langle g \rangle : X \equiv 0 \pmod 3\}$

note that $1 \notin S_1$

The algorithm is as follows:

$T:=1$, $\alpha=0$, $\beta=0$

$(H,\gamma,\delta):=(T,\alpha,\beta)$

$i:=0$;

do {

$i{+}{+}$

$(T,\alpha,\beta):=f(T,\alpha,\beta)$

$(H,\gamma,\delta):=f(f(H,\gamma,\delta))$

} while $(T\neq H \mod p)$

$T=g^{\alpha}y^{\beta}$

$H=T$

now $T=H \pmod p$

$$g^{\alpha}y^{\beta}=g^{\gamma}\cdot y^{\delta} \pmod p$$

$$g^{\alpha}(g^{x})^{\beta}=g^{\gamma}\cdot (g^{x})^{\delta} \pmod p$$

$$g^{\alpha+x\beta}=g^{\gamma+x\delta} \pmod p$$

$$\alpha+x\beta=\gamma+x\delta \pmod{\underbrace{\mathrm{ord}\, g}_{=q\ \text{(prime)}}}$$

$$\alpha-\gamma=(\delta-\beta)x \pmod q$$

if $\delta\neq\beta \mod q$ then we can calculate

$$\underline{\underline{x=(\alpha-\gamma)\cdot(\delta-\beta)^{-1} \pmod q}}$$

if $\delta=\beta \pmod q$ then we start again with random α,β and $T=g^{\alpha}y^{\beta}$

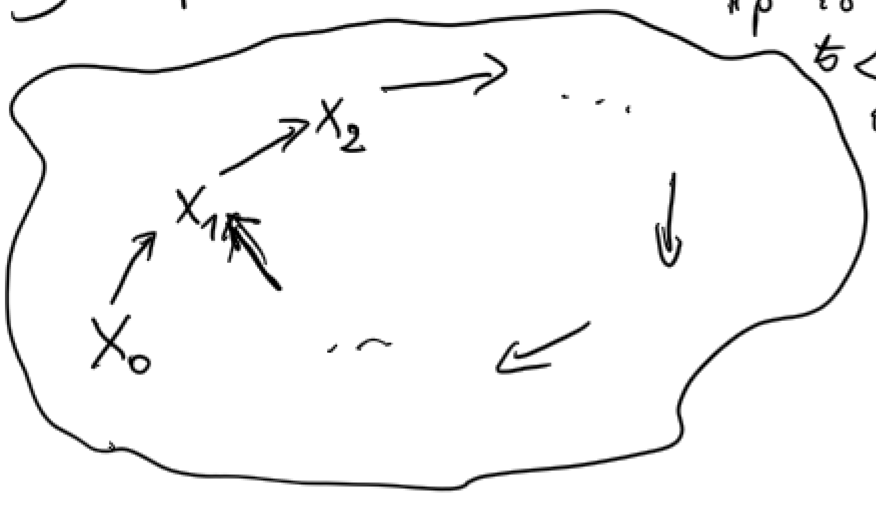
So we have to keep track on $(T,\alpha,\beta),(H,\gamma,\delta)$ to find x.

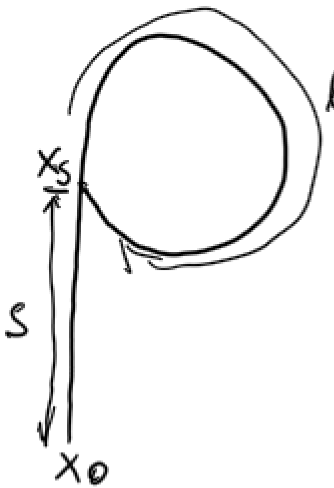
Why the algorithm stops? and how many steps it takes?

$\mathbb{F}_p^*$ is finite so $\langle g\rangle$ is as well

$T=X_i$

$H=X_{2i}$





l – length of the period

$X_s = X_{s+l}$

$s \geq 0$

the tortoise T must pass X_s ~~to~~ enter the loop, but the hare is already on the loop.

When both T and H are on the loop, the distance between them decreases by <u>one</u> in each iteration

(tortoise – one application of f, hare – 2 applications of f)
difference → one ~~a~~ application of f.

so for $i \geq s$ we have $T = H$
for $i < s+l$

if the collision did not occur for $i = s$ it means that the distance between H and T is smaller than l, so the hare will catch up the tortoise ~~aft~~ in the number of smaller than l.

if the collision occurred for $i = s$ then $l = 0$.

Finally: $s \leq i < s+l$.

How large is $s+l$?

we count for $s+l = O(\sqrt{\operatorname{ord} g})$ ← from birthday paradox

{ please keep track on i during computations and print it

$\operatorname{ord} g = \tilde{p} = q$

ord $\hat{g} = \hat{p}$

$p = 2\tilde{p} + 1$

$\tilde{g} = g^2 \pmod{p}$

$p, \tilde{p}$ - are prime

$\mathbb{F}_p^* \cong C(2) \oplus C(\tilde{p})$

$|\mathbb{F}_p^*| = p - 1 = 2\tilde{p}$

$g \to (g_2, g_{\tilde{p}})$

ord $g_2 = 2$

ord $g_{\tilde{p}} = \tilde{p}$

$\tilde{g} = g^2 \to (g_2^2, g_{\tilde{p}}^2) = (1, g_{\tilde{p}}^2) \neq I = (1,1)$

$g_{\tilde{p}}^2 \neq 1$

$\tilde{g} = (g^2) \pmod{p}$

$\underbrace{\tilde{g}^1, \tilde{g}^2, \dots, 1}_{q}$

q - length of sequence

Let K be a field.

let 1 - neutral element of $\cdot$ $\quad 1 \in F \setminus \{0\}$

let 0 - neutral element of $+$

1

$1+1$

$1+1+1$

$\dots$

$1+1+1+\dots+1$

$\dots$

if the sequence of results does not contain 0, then we say that the characteristic of K is 0. Otherwise, the characteristic of K is positive — always a prime number:

$\underbrace{1+1+\dots+1}_{\text{char } K} = 0$ ← it is always a prime number.