Pollard's rho discrete logarithm algorithm

- Pollard rho discrete logarithm algorithm (1978)
  compute integers s and t such that $\beta^s = \alpha^t$
  - partition the group G into three roughly equal-sized set S_1, S_2 and S_3. Let $x_0 = 1_G$ and x_0 is not in S_2

$$x_{i+1} = \begin{cases} \beta\, x_i & for\ \ x_i \in S_1 \\ x_i^{\ 2} & for\ \ x_i \in S_2 \\ \alpha\, x_i & for\ \ x_i \in S_3 \end{cases}$$

Let $x_i = \beta^{a_i} \alpha^{b_i}$

$$a_{i+1} = \begin{cases} a_i + 1 \pmod{n} & for \;\; x_i \in S_1 \\ 2a_i \pmod{n} & for \;\; x_i \in S_2 \\ a_i & for \;\; x_i \in S_3 \end{cases}$$

$$b_{i+1} = \begin{cases} b_i & for \;\; x_i \in S_1 \\ 2b_i \pmod{n} & for \;\; x_i \in S_2 \\ b_i + 1 \pmod{n} & for \;\; x_i \in S_3 \end{cases}$$

where n = p-1 when G = Z^*_p

We should expect some integer i=O($n^{1/2}$) such that

$x_i = x_{2i}$, then this gives $\beta^s = \alpha^t$ (using Floyd's algorithm)

with $s = a_i - a_{2i} \pmod n$ $t = b_{2i} - b_i \pmod n$

If $\gcd(s, n) = 1$

then compute $s^{-1} \pmod n$

and we have $\beta = \alpha^{s^{-1}t}$, so that $\log_\alpha \beta = s^{-1}t \pmod n$.

If $\gcd(s, n) = d > 1$

little work to do... (Omitted)

- Floyd’s cycle-finding algorithm:

  One starts with the pair (x_1, x_2), and iteratively computes (x_i, x_{2i}) from the previous (x_{i-1}, x_{2i-2}), until $x_m=x_{2m}$ for some m. The expected running time of this method is $O(n^{1/2})$.

- Pollard's rho algorithm for discrete logarithms
  - INPUT: a generator α of a cyclic group G and β is an element of G
  - OUTPUT: $\log_g a$

    1. Set $x_0 \leftarrow 1$, $a_0 \leftarrow 0$, $b_0 \leftarrow 0$
    2. For i = 1, 2, …. Do the following:

       2.1 Use x_{i-1}, a_{i-1}, b_{i-1} to compute x_i, a_i, b_i
       Use x_{2i-2}, a_{2i-2}, b_{2i-2} to compute x_{2i}, a_{2i}, b_{2i}

       2.2 if $x_i = x_{2i}$, then do the following
       set $r \leftarrow b_i - b_{2i}$
       if $\gcd(r,n) \neq 1$ then return 'failure'
       else return $r^{-1}(a_{2i} - a_i) \bmod n$

- Example:
  $\alpha = 2$ is a generator of the subgroup G of $Z_{383}{}^{*}$ of order n= 191.(in this case $<\alpha> = G \neq Z_{383}{}^{*}$)

  Suppose $\beta = 228$. Find $\log_2 228$.

  Solution:

  Partition G into 3 subsets, let

$$S_1 = \{x \in G \mid x = 1 \bmod 3\}$$

$$S_2 = \{x \in G \mid x = 0 \bmod 3\}$$

$$S_3 = \{x \in G \mid x = 2 \bmod 3\}$$

i	x_i	b_i	a_i	x_{2i}	b_{2i}	a_{2i}
1	228	0	1	279	0	2
2	279	0	2	184	1	4
3	92	0	4	14	1	6
4	184	1	4	256	2	7
5	205	1	5	304	3	8
6	14	1	6	121	6	18
7	28	2	6	144	12	38
8	256	2	7	235	48	152
9	152	2	8	72	48	154
10	304	3	8	14	96	118
11	372	3	9	256	97	119
12	121	6	18	304	98	120
13	12	6	19	121	5	51
14	144	12	38	144	10	104

- Solution (continued):

From the table, we have $x_{14} = x_{28} = 144$.

Finally compute

$$(b_{28} - b_{14}) / (a_{14} - a_{28}) \bmod 191$$

$$= (-2)/(-66) \bmod 191$$

$$= 1/33 \bmod 191$$

$$= 110 \bmod 191.$$

Hence, $\log_2 228 = 110$.