Algorithm 5.9: POLLARD RHO FACTORING ALGORITHM(n, x_1)

```
external f
x ← x_1
x' ← f(x) mod n
p ← gcd(x − x', n)
while p = 1
       ⎧ comment: in the ith iteration, x = x_i and x' = x_2i
       ⎪ x ← f(x) mod n
  do   ⎨ x' ← f(x') mod n
       ⎪ x' ← f(x') mod n
       ⎩ p ← gcd(x − x', n)
if p = n
  then return ("failure")
  else return (p)
```

Example 5.10 Suppose that $n = 7171 = 71 \times 101$, $f(x) = x^2 + 1$ and $x_1 = 1$. The sequence of x_i's begins as follows:

1	2	5	26	677	6557	4105
6347	4903	2218	219	4936	4210	4560
4872	375	4377	4389	2016	5471	88

x_7 x_{18}

The above values, when reduced modulo 71, are as follows:

1	2	5	26	38	25	58
28	4	17	6	37	21	16
44	20	46	58	28	4	17

The first collision in the above list is

$$x_7 \bmod 71 = x_{18} \bmod 71 = 58.$$

$\gcd(x_{18} - x_7, 7171) = 71$

$x_{18} - x_7 = 284$

The Pollard Rho Discrete Logarithm Algorithm

$\log_\alpha \beta$ in Z_n

G

Let $S_1 \cup S_2 \cup S_3$ be a partition of G into three subsets of roughly equal size. We define a function $f : \langle \alpha \rangle \times \mathbb{Z}_n \times \mathbb{Z}_n \to \langle \alpha \rangle \times \mathbb{Z}_n \times \mathbb{Z}_n$ as follows:

$$f(x, a, b) = \begin{cases} (\beta x, a, b+1) & \text{if } x \in S_1 \\ (x^2, 2a, 2b) & \text{if } x \in S_2 \\ (\alpha x, a+1, b) & \text{if } x \in S_3. \end{cases}$$

$$(x, a, b) \longleftrightarrow x = \alpha^a \beta^b$$

$$(x_i, a_i, b_i) = \begin{cases} (1, 0, 0) & \text{if } i = 0 \\ f(x_{i-1}, a_{i-1}, b_{i-1}) & \text{if } i \geq 1. \end{cases}$$

Algorithm 6.2: POLLARD RHO DISCRETE LOG ALGORITHM(G, n, α, β)

```
procedure f(x, a, b)
  if x ∈ S₁
    then f ← (β · x, a, (b + 1) mod n)
    else if x ∈ S₂
    then f ← (x², 2a mod n, 2b mod n)
    else f ← (α · x, (a + 1) mod n, b)
  return (f)

main
  define the partition G = S₁ ∪ S₂ ∪ S₃
  (x, a, b) ← f(1, 0, 0)
  (x', a', b') ← f(x, a, b)
  while x ≠ x
       ⎧ (x, a, b) ← f(x, a, b)
    do ⎨ (x', a', b') ← f(x', a', b')
       ⎩ (x', a', b') ← f(x', a', b')
  if gcd(b' − b, n) ≠ 1
    then return ("failure")
    else return ((a − a')(b' − b)⁻¹ mod n)
```

We compare the triples (x_{2i}, a_{2i}, b_{2i}) and (x_i, a_i, b_i) until we find a value of $i \geq 1$ such that $x_{2i} = x_i$. When this occurs, we have that

$$\alpha^{a_{2i}} \beta^{b_{2i}} = \alpha^{a_i} \beta^{b_i}.$$

If we denote $c = \log_\alpha \beta$, then it must be the case that

$$\alpha^{a_{2i} + c b_{2i}} = \alpha^{a_i + c b_i}.$$

Since α has order n, it follows that

$$a_{2i} + c b_{2i} \equiv a_i + c b_i \pmod{n}.$$

This can be rewritten as

$$c(b_{2i} - b_i) \equiv a_i - a_{2i} \pmod{n}.$$

If $\gcd(b_{2i} - b_i, n) = 1$, then we can solve for c as follows:

$$c = (a_i - a_{2i})(b_{2i} - b_i)^{-1} \bmod n.$$

Example 6.3 The integer $p = 809$ is prime, and it can be verified that the element $\alpha = 89$ has order $n = 101$ in $\mathbb{Z}_{809}^*$. The element $\beta = 618$ is in the subgroup $\langle\alpha\rangle$; we will compute $\log_\alpha \beta$.

Suppose we define the sets S_1, S_2 and S_3 as follows:

$$S_1 = \{x \in \mathbb{Z}_{809} : x \equiv 1 \pmod 3\}$$

$$S_2 = \{x \in \mathbb{Z}_{809} : x \equiv 0 \pmod 3\}$$

$$S_3 = \{x \in \mathbb{Z}_{809} : x \equiv 2 \pmod 3\}.$$

For $i = 1, 2, \ldots$, we obtain triples (x_{2i}, a_{2i}, b_{2i}) and (x_i, a_i, b_i) as follows:

i	(x_i, a_i, b_i)	(x_{2i}, a_{2i}, b_{2i})
1	(618, 0, 1)	(76, 0, 2)
2	(76, 0, 2)	(113, 0, 4)
3	(46, 0, 3)	(488, 1, 5)
4	(113, 0, 4)	(605, 4, 10)
5	(349, 1, 4)	(422, 5, 11)
6	(488, 1, 5)	(683, 7, 11)
7	(555, 2, 5)	(451, 8, 12)
8	(605, 4, 10)	(344, 9, 13)
9	(451, 5, 10)	(112, 11, 13)
10	(422, 5, 11)	(422, 11, 15)

The first collision in the above list is $x_{10} = x_{20} = 422$.

$$c = (11 - 5)(11 - 15)^{-1} \bmod 101 = (6 \times 25) \bmod 101 = 49.$$

Therefore, $\log_{89} 618 = 49$ in the group $\mathbb{Z}_{809}^*$.