```
> restart; path:="": #"J:\\eos.ncsu.
  edu/users/k/kaltofen/www/courses/ComputAlgebra/Maple/":
  read(cat(path,"new_pollard_rho.mpl")):
```

```
> Nxt:=proc(x) x+3 mod n; end;
```

$$Nxt := \mathbf{proc}(x)\ x + 3\ \mathbf{mod}\ n\ \mathbf{end\ proc} \tag{1}$$

```
> Equ:=proc(x,y) x=y; end;
```

$$Equ := \mathbf{proc}(x, y)\ x = y\ \mathbf{end\ proc} \tag{2}$$

```
> n:=17;
```

$$n := 17 \tag{3}$$

```
> printlevel:=1;
```

$$printlevel := 1 \tag{4}$$

```
> cycle_indices(7,Nxt,Equ);
```

"n = ", 17

[0, 17] (5)

```
> cycle_indices(7,Nxt,Equ,'return_mu_lambda'=false);
```

"n = ", 17

[17, 34] (6)

```
> n := ithprime(100); Nxt2:=proc(x) x^2+1 mod n; end;
```

$$n := 541$$

$$Nxt2 := \mathbf{proc}(x)\ x\text{^}2 + 1\ \mathbf{mod}\ n\ \mathbf{end\ proc} \tag{7}$$

```
> `help/text/cycle_indices`;
```

TEXT (FUNCTION: cycle_indices - compute the lengths of preperiod and period,
of a user supplied function, ,
CALLING SEQUENCES: cycle_indices(x0, fn, eq), ,
PARAMETERS: x0 - a starting value, fn - a single argument function,
eq - an equality test, , SYNOPSIS: ,
- The call cycle_indices(x0, fn, eq) returns a pair [mu, lambda],
where mu is the length of the preperiod and lambda is the,
length of the period of the sequence x0, fn(x0), fn(fn(x0)),...,
where equality is tested by the function eq, , EXAMPLE: ,
> nxt := proc(x) x^2 + 1 mod 101; end:, > eq := proc(x, y) x = y; end:,
> cycle_indices(3, nxt, eq):, , [12, 9]) (8)

```
> cycle_indices(3,Nxt2,Equ,'return_mu_lambda'=false);
```

"n = ", 13

[13, 26] (9)

```
> cycle_indices(100,Nxt2,Equ);
```

"n = ", 13

[0, 13] (10)

```
> p1:=ithprime(100);
```

$$p1 := 541 \tag{11}$$

```
> p2:=ithprime(10);
```

$$p2 := 29 \tag{12}$$

```
> q := p1*p2;
```

$$q := 15689 \tag{13}$$

```
> pollard_rho(q,100);
GCD =29
```

"n = ", 12
29 **(14)**

```
> q2:=31*47;
```

$$q2 := 1457 \quad \textbf{(15)}$$

```
> pollard_rho(q2,11);
GCD =31
```

"n = ", 3
31 **(16)**

```
> q3:=97^3;
```

$$q3 := 912673 \quad \textbf{(17)}$$

```
> printlevel:=2: pollard_rho(q3);
```

[3, 912673]
"X=", [10, 912673], "Y=", [101, 912673]
"X=", [101, 912673], "Y=", [36083, 912673]
"X=", [10202, 912673], "Y=", [727505, 912673]
"X=", [36083, 912673], "Y=", [359965, 912673]
"X=", [511192, 912673], "Y=", [683973, 912673]
"X=", [727505, 912673], "Y=", [19211, 912673]

```
GCD =97
```

"equal_side_effect:", *GCD*, " := ", 97
"n = ", 6
97 **(18)**

```
> printlevel:=0:
  # search for equal collision lengths
  for i from 10 to 50 do
      n:=ithprime(i); print(n,cycle_indices(3,Nxt2,Equ,
  'return_mu_lambda'=false));
  od:
```

29, [6, 12]
31, [3, 6]
37, [2, 4]
41, [7, 14]
43, [5, 10]
47, [3, 6]
53, [6, 12]
59, [9, 18]
61, [10, 20]
67, [3, 6]
71, [5, 10]
73, [6, 12]
79, [7, 14]
83, [15, 30]
89, [14, 28]
97, [6, 12]
101, [18, 36]
103, [14, 28]
107, [14, 28]
109, [14, 28]
113, [6, 12]

127, [8, 16]
131, [7, 14]
137, [17, 34]
139, [25, 50]
149, [14, 28]
151, [6, 12]
157, [3, 6]
163, [12, 24]
167, [8, 16]
173, [8, 16]
179, [21, 42]
181, [14, 28]
191, [15, 30]
193, [14, 28]
197, [4, 8]
199, [6, 12]
211, [12, 24]
223, [5, 10]
227, [23, 46]
229, [28, 56] **(19)**

```
> pollard_rho(83*191);
  pollard_rho(83*191,5); # start at different residue
```

```
GCD =15853
```

15853

```
GCD =83
```

83 **(20)**

```
> n:=(9485391712037823777737 3/11); printlevel:=1: pollard_rho(n);
  ifactor(n);
```

$n := 8623083374579839797943$

```
GCD =2641812997
```

"n = ", 26828
2641812997
(3264077883019) (2641812997) **(21)**

```
> read(cat(path,"new_discrete_log.mpl")):
```

```
> p := ithprime(1000000); with(numtheory): primroot(p); rnd := rand
  (0..p-1): printlevel:=1:
```

$p := 15485863$
6 **(22)**

```
> printlevel:=1:
  for i from 1 to 3 do discrete_log(29,6,p,rnd(),rnd(),p-1); printf
  ("%s","_____");od;
```

"Collision: ", [10858238, 29, 6, 15485863, 10087279, 7140996], [10858238, 29, 6, 15485863, 10545457, 2896518]
"Failure:", $-(2)(3)(7)(10909)$, "ord=", $(2)(3)(7)^2(52673)$, "gcd = ", 42
"Recursive continuation with", 13916181, 9219709, 15485863, "init = ", 9550684, 11443958, "ord =", 42
"Collision: ", [1924698, 13916181, 9219709, 15485863, 39, 37], [1924698, 13916181, 9219709, 15485863, 17, 39]
"Failure:", (2) (11), "ord=", (2) (3) (7), "gcd = ", 2

"Iterative continuation with", 15485862, 15485862, 15485863, "ord =", 2
"n = ", 12
"n = ", 4852
8778231

"Collision: ", [13694395, 29, 6, 15485863, 7352278, 6499336], [13694395, 29, 6, 15485863, 15265660, 15462388]

"Failure:", $-(2)(3)(1318897)$, "ord=", $(2)(3)(7)^2(52673)$, "gcd = ", 6
"Iterative continuation with", 15485862, 103145, 15485863, "ord =", 6
"n = ", 4852
8778231

"Collision: ", [6634482, 29, 6, 15485863, 3400816, 9628076], [6634482, 29, 6, 15485863, 6776326, 7630892]

"Failure:", $-(2)(3)(5)(37)(3041)$, "ord=", $(2)(3)(7)^2(52673)$, "gcd = ", 6
"Iterative continuation with", 15485862, 103145, 15485863, "ord =", 6
"n = ", 4852
8778231

```
> 6 &^ 8778231 mod p;
```


(23)