A2Q4

Let p be a prime and let $0 < x_1 < p$. Suppose we compute the sequence $x_{n+1} = x_n^2$ modulo p for n = 1, 2, 3, ... Then since the values in the sequence remain in the range [1,p-1] we must get into a cycle.

Write a Maple procedure cycle (x,p) that outputs the period π of the cycle, that is, the number of integers in the cycle.

```
> restart:
> cycle := proc(x,p)
      local running, L, k, result;
      running := x mod p;
      L := [];
      while not member(running, L, 'k') do
          L := [op(L), running];
          running := running^2 mod p;
      od;
      result := nops(L)-k+1;
      end:
> cycle(10,13);
```

2 **(1)**

```
> seq(cycle(x,37), x=1..36);
```

1, 6, 6, 6, 6, 1, 6, 2, 6, 2, 2, 6, 6, 2, 6, 6, 6, 6, 6, 6, 6, 6, 2, 6, 6, 2, 2, 6, 2, 6, 1, 6, 6, 6, 6, 1 **(2)**

```
> cycle(5,997);
```

82 **(3)**