Ejercicio 4

March 4, 2018

```
In [3]: def orden(M,p):
            for i in xsrange(1,p):
                if power_mod(M,i,p) == 1:
                    return i
            return -1

In [5]: orden(10,13)

Out[5]: 6

In [105]: def fuerza_bruta(p,M,MC):
              MC = mod(MC,p)
              for i in xsrange(1,p):
                  if power_mod(M,i,p) == MC:
                      return i
              return -1

In [106]: fuerza_bruta(13,10,10)

Out[106]: 1

In [107]: def baby_giant(p,M,MC):
              MC = mod(MC,p)
              c = ceil(sqrt(p))
              L = [power_mod(M,j,p)for j in xsrange(c)]
              m = power_mod(M,-c,p)
              for i in xsrange (p):
                  if (MC*m^i) in L:
                      return c*i + L.index(MC*m^i)
              return -1

In [108]: baby_giant(13,10,10)

Out[108]: 1

In [118]: p = next_prime(10^5)
          M = randint(2,p-1)
          P = [i for i in xsrange(2,p-1) if gcd(i,p-1) == 1]
```

```
In [140]: %time
          baby_giant(p,M,M^P[15])

CPU times: user 0 ns, sys: 0 ns, total: 0 ns
Wall time: 17.9 µs


Out[140]: 59

In [141]: %time
          print fuerza_bruta(p,M,M^P[15])

CPU times: user 0 ns, sys: 0 ns, total: 0 ns
Wall time: 15 µs
59


In [ ]:
```