MR Bugiardi

Lorenzo Livio Vaccarecci (matr. 5462843)

A.A. 2023/2024

1 Codice

```python
import math
import random

def MCPrimalityTest(n, a=None):
  s = 0
  q = n - 1
  while q % 2 == 0:
    s += 1
    q //= 2
  if a is None:
      a = random.randint(2,n-2)
  x = pow(a, q, n)
  if x == 1 or x == n-1:
    return "Probabilmente primo"
  i = s
  while i-1 >= 0:
    x = pow(x, 2, n)
    if x == n-1:
      return "Probabilmente primo"
    i -= 1
  return "Probabilmente composto", s, q

def MCD(a, b):
    while b:
        a, b = b, a % b
    return a

def Z(n):
  return [a for a in range(1,n) if MCD(a,n) == 1]

def H(n):
  return [a for a in Z(n) if pow(a,n-1,n) == 1]

carmichael = [561,1105,1729,2465,2821,6601,8911]
for n in carmichael:
  primality = MCPrimalityTest(n)
  Hn = H(n)
  print(f"I bugiardi per {n}({len(Hn)}) sono {Hn}")
  print(f"Zn, Hn uguali? {Z(n) == Hn}")
```

Sappiamo che per i numeri di Carmichael i bugiardi sono i coprimi e per sicurezza controllo se Hn è uguale ai coprimi.

- I bugiardi per **561** sono tutti i numeri da 1 a 560 tranne tutti i multipli di [3,11,17] (compresi)
- I bugiardi per **1105** sono tutti i numeri da 1 a 1104 tranne tutti i multipli di [5,13,17] (compresi)
- I bugiardi per **1729** sono tutti i numeri da 1 a 1728 tranne tutti i multipli di [7,13,19] (compresi)
- I bugiardi per **2465** sono tutti i numeri da 1 a 2464 tranne tutti i multipli di [5,17,29] (compresi)
- I bugiardi per **2821** sono tutti i numeri da 1 a 2820 tranne tutti i multipli di [7,13,31] (compresi)
- I bugiardi per **6601** sono tutti i numeri da 1 a 6600 tranne tutti i multipli di [7,23,41] (compresi)
- I bugiardi per **8911** sono tutti i numeri da 1 a 8910 tranne tutti i multipli di [7,19,67] (compresi)