ESERCIZIO 3

Lavoro svolto da:
-Magno Alessandro : 4478234

Svolgimento

Verifica piccolo teorema di Fermat per n = 7:

7 è primo e preso ad esempio un a=2 intero, il quale non è divisibile per 7

$$a^n = a\ (mod\ n)$$

$$2^7 = (1+1)^7 = 1 + \binom{7}{1} + \cdots + \binom{7}{6} + 1 = 1 + 0 + \cdots + 0 + 1 = 2\ (mod\ 7)$$

Verifica piccolo teorema di Fermat per n = 9 con a = 2:

$$2^9 = (1+1)^9 = 1 + \binom{9}{1} + \cdots + \binom{9}{8} + 1 = 1 + 0 + \cdots + 0 + 1 = 2\ (mod\ 9)$$

Implementazione test Miller-Rabin:

```python
def MCMillerRabinTest(n,q,a):
    s = 0
    while(q%2==0):
        s = s + 1
        q = q / 2

    x = (a**q) % n

    if x == 1%n or x == -1%n:
       return("n forse primo")
    else:
        while(s-1>=0):
            x = (x**2) % n
            if x == -1%n:
                return("n forse primo")
            s = s-1
        return("n è composto")

def main():
    n1 = 7
    n2 = 9
    q1 = n1-1
    q2 = n2-1
    for a in range(2,6):
        print(MCMillerRabinTest(n1,q1,a))

    for a in range(2,8):
        print(MCMillerRabinTest(n2,q2,a))
main()
```

esempio con n = 7 , a = 2

s = 0

q = n-1 = 6

while(q pari) {

    s = s+1=1

    q = q/2 = 3

    //il ciclo si ferma al primo giro, q dispari

}

a = 2

x = a^q (mod n) = 2^3 (mod 7) = 1

if x = $\pm$1 // si x = 1

  “7 forse è primo”

I risultati ottenuti per n = 7 e a = 2,3,4,5 sono “n forse è primo” per tutti i valori di a. Infatti per il teorema di Fermat il MCMillerRabinTest non dichiara mai composto un numero primo.

Mentre per n = 9 e a = 2,3,4,5,6,7 si ottiene “n è composto” per tutti i valori di a. Quindi tutti i possibili valori di a {2,..7(n-2)} sono testimoni di Miller-Robin.