HW5 - Mersenne Prime

(정수론)

18013195

정보보호학과

이풍원

1) lucas_lehmer_test(p): it tests whether the Mersenne number M_p = 2^p - 1 is prime or not where p is a prime by using the Lucas-Lehmer test. It outputs 1 if it is prime or 0 otherwise.

```
16  def lucas_lehmer_test (p):
17      if(p==2): return 1
18      r_1=4 # k>=2
19      M_p=(2**p)-1
20
21      for i in range(2,p):
22          r_1=(r_1**2-2)%M_p
23          if r_1==0:
24              return 1
25      return 0
```

17 행: p 가 2 이면 메르센소수이기 때문에 1 을 반환한다.

18~19 행: r_1 의 초기값은 4, M_p 의 초기값은 2^p -1 로 저장한다.

21 행: p-1 까지 반복한다.

22 행: r_1 에 r_1^2 -2 mod M_p 를 저장한다

23~24 행: p-1 까지 반복하면서 r_1 이 0 이되면 메르센소수이기 때문에 1 을 반환한다.

25 행: 위의 p-1 까지 반복하여 만족하지 않으면 메르센소수가 아니기 때문에 0 을 반환한다.

2) find_mersenne_primes(max): it prints all Mersenne primes from 3 to the Mersenne number M_{max} by using the lucas_lehmer_test function and generate_all_primes function (in previous homework). Note that it only prints primes p for M_p = 2^p - 1.

```
27  def find_mersenne_primes(max):
28      mersenneList=[]
29      for i in generate_all_primes(max):
30          if lucas_lehmer_test(i):
31              mersenneList.append(i)
32      return mersenneList
```

28 행: 메르센소수를 담을 list 로 선언

29 행: generate_all_primes 에 max 을 넣어 max 까지의 소수를 반환하여 i 에 넣어 그 개수 만큼 반복한다.

30~31 행: lucas_lehmer_test 에 소수인 i 값을 넣어 메르센소수이면 mersenneList 에 append 하여 저장한다.

32 행: 메르센소수들을 반환한다.

3) main 및 실행 결과

```
34  number=[3,17,31,521,9689,9697]
35  for i in number:
36      print("lucas_lehmer_test(",i,") = ",lucas_lehmer_test(i))
37
38  print("find_mersenne_primes(5000)=",find_mersenne_primes(5000))
```

```
문제   출력   디버그 콘솔   터미널
PS C:\Users\vnddn\OneDrive\바탕 화면\js> & C:/Users/vnddn/AppData/Local/Programs/Python/Python39/python.exe "c:/Users/vnddn/OneDri
lucas_lehmer_test( 3 ) =  1
lucas_lehmer_test( 17 ) =  1
lucas_lehmer_test( 31 ) =  1
lucas_lehmer_test( 521 ) =  1
lucas_lehmer_test( 9689 ) =  1
lucas_lehmer_test( 9697 ) =  0
find_mersenne_primes(5000)= [2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423]
```