Homework Assignment 04

Machiry Aravind Kumar

UCSB

1 Implement the Fermats primality testing algorithm in Python, C++ or Mathematica, and apply to these numbers and discover the smallest liar and smallest witness for each one. What is the property of the witness?

I implemented the algorithm in python. File `machiry_hw4.py` has the code for the algorithm. I used Montgomery exponentiation to perform $a^{p-1}modn$ check. The results for smallest witness and smallest liar for the given numbers are as shown in Table 1.

Target Number	Smallest Witness	Smallest Liar
41041	7	2
62745	3	2
63973	7	2
75361	11	2
101101	7	2
126217	7	2
172081	7	2
188461	7	2
278545	5	2
340561	13	2
449065	5	2
552721	13	2
656601	3	2
658801	11	2
670033	7	2
748657	7	2
838201	7	2
852841	11	2
997633	7	2
1033669	7	2
1082809	7	2
1569457	17	2
1773289	7	2
2100901	11	2
2113921	19	2
2433601	17	2
2455921	13	2

The property of smallest witness of all these numbers are they are the **smallest prime factors of corresponding carmichael numbers**.

2 Implement the Miller-Rabin primality testing algorithm in Python, C++ or Mathematica, and apply to these numbers and discover the smallest liar and smallest witness for each one.

I implemented the algorithm in python. File `machiry_hw4.py` has the code for the algorithm. I used Montgomery exponentiation to perform all modular exponentiations. The results for smallest witness and smallest liar for the given numbers are as shown in Table 2.

Target Number	Smallest Witness	Smallest Liar
41041	2	16
62745	2	16
63973	2	9
75361	2	256
101101	2	16
126217	2	16
172081	2	9
188461	2	9
278545	2	98
340561	2	35
449065	2	16
552721	2	21
656601	2	16
658801	2	101
670033	2	9
748657	2	9
838201	2	9
852841	2	16
997633	2	898
1033669	2	9
1082809	2	16
1569457	2	256
1773289	2	3
2100901	2	16
2113921	2	195
2433601	2	98
2455921	2	9