CSC 372
Fall 2022
Assignment #3 - Number of Witnesses

The purpose of this assignment is to verify the claim that most numbers will be witnesses for a given composite value. [Recall “witness” refers to a value that the Miller-Rabin Test can use to tell that a number is not prime.]

Read *n* from the file "witness.in". You may assume *n* fits in a 64-bit signed integer. You may assume *n* fits in a 32-bit signed integer if *n* is not prime.

Pseudocode for program

```
while (n > 2)

    • If n is prime, print the value of n and "is prime" to the file "witness.out"
    • otherwise (n is not prime)
        o Count the number of witnesses that n is not prime from 2 to n − 2.
        o Print to "witness.out" the value of n, a space, and the number of numbers
          from 2 to n − 2 that are not witnesses.
    • Read the next n from the file "witness.in".
```

You should see that the number of witnesses for a composite number is usually the vast majority of the numbers from 2 to $n - 2$. This fact makes the Miller-Rabin primality test a very accurate one.

Submit your program using D2L by midnight on Friday, December 2nd.

This is a small program and should be an individual effort.

A sample input file and sample output file are posted. Be sure to do a file compare of your output file and the sample. Note that the instructor’s solutions takes under 2 seconds to process the sample file.

Sample Input file	Sample Output file
20 25 29 1642591 1645291 -1	20 0 25 2 29 is prime 1642591 28 1645291 is prime

Note that the number of values that are not witnesses for the sample is very low, as expected.