Assignment 21

Due by class time Tuesday, December 13

1. Write a Python program called **shorFactor(*N*)** that takes an integer $N > 1$ as input, which you can assume will not be prime, and uses Shor's algorithm to find the factors. The outline of Shor's algorithm that we discussed in class is given below:

   (a) pick a random integer a such that $1 < a < N$

   (b) if a and N are not co-prime, compute $g = \text{GCD}(a, N)$ and N/g as the factors, and stop.

   (c) otherwise, determine the period r of the function $f_{a,N}(x) = a^x \bmod N$

   (d) if the period is odd, go back to step (a)

   (e) compute $s = a^{\frac{r}{2}} \bmod N$

   (f) if $s = N - 1$ (equivalent to $-1 \bmod N$), go back to step (a)

   (g) otherwise, compute $\text{GCD}(s + 1, N)$ and $\text{GCD}(s - 1, N)$ as the factors, and stop.

   Here are some additional Python definitions that will be useful:

```
def GCD(a, b):
    while b > 0:
        remainder = a % b
        a = b
        b = remainder
    return a

def coprime(a, N):
    return GCD(a, N) == 1

def findPeriod(a, N):
    if not coprime(a, N):
        print("Sorry,", a, "and", N, "must be coprime")
        return
    for x in range(1, N):
        if powermod(a, x, N) == 1:
            return x
```

   You can use the **findPeriod** function above, along with your **powermod** function from the previous assignment, to determine the period in step (c). Your program should also report what it's doing in each step, so the user can follow the process. Some sample output is shown below for the numbers 371 and 247:

```
>>> shorFactor(371)
chose a = 15
15 and 371 are co-prime
function f is 15^x mod 371
period of f is 13
period is odd...trying again
chose a = 18
18 and 371 are co-prime
function f is 18^x mod 371
period of f is 156
s = 211 mod 371
GCD(212, 371) = 53
GCD(210, 371) = 7
factors of 371 are 53 and 7

>>> shorFactor(247)
chose a = 117
117 and 247 are not co-prime
factors are 13 and 19

>>> shorFactor(247)
chose a = 181
181 and 247 are co-prime
function f is 181^x mod 247
period of f is 18
s = 246 mod 247
s is equivalent to -1 mod 247...trying again
chose a = 175
175 and 247 are co-prime
function f is 175^x mod 247
period of f is 36
s = 77 mod 247
GCD(78, 247) = 13
GCD(76, 247) = 19
factors of 247 are 13 and 19
```

2. Use your **shorFactor** program to factor the following numbers:
   - $N = 474577$
   - $N = 3937361$
   - $N = 5573899$