Homework 6

Due **Saturday**, October 23

Implementation Part

1. Implement Pollard's $p-1$ algorithm to factor large numbers. Explicitly, define an algorithm `PollardFactor(N,a = 2,n = infinity)` which attempts to factor N by computing the gcd of $a^{i!}-1$ and N for $i \leq n$. It should default to computing factorial powers of 2, and should default to running forever if you don't specify an upper bound (this is probably bad practice in general but is useful if you don't have a particular upper bound in mind and just want to have it run for a while to see if you can find a factorization). Make sure to include an appropriate response if your algorithm ever computes $\gcd(a^{i!}, N) = N$. **Note:** It is important that every step in this algorithm be as streamlined as possible, eliminating any redudant computations to give the best possible chance of factoring a large number.

2. Use your algorithm from part 1 to try and factor the following numbers. (You might want an upper bound for the last few).

   (a) N = 13927189

   (b) N = 168441398857

   (c) N = 47317162267924657513

   (d) N = 523097775055862871433433884291

   (e) N = 515459117588889238503625135159

3. Let's gather some data on the prime number theorem and related things. We will be using your function `probablyPrime` from the first takehome assignment.

   (a) Write a function `pi(n)` which computes
   $$\pi(n) := \#\{\text{primes } p \text{ such that } p \leq n\}.$$

   (b) Compute the ratio $\pi(n)/(n/\ln n)$ for $n = 10, 100, 1000, 10000$, and 100000. Does this make you believe in the prime number theorem? (Note: sage has a built in function `ln(x)`, but you may need to cast your output as a float to see a decimal expansion of the output.)

   (c) Write functions `pi1(n)` and `pi3(n)` which compute
   $$\begin{aligned} \pi_1(n) &:= \#\{\text{primes } p \text{ such that } p \leq n \text{ and } p \equiv 1 \mod 4\}, \\ \pi_3(n) &:= \#\{\text{primes } p \text{ such that } p \leq n \text{ and } p \equiv 3 \mod 4\}, \end{aligned}$$
   respectively.

   (d) Compute the ratio $\pi_1(n)/\pi_3(n)$ for $n = 10, 100, 1000, 10000$, and 100000. Make a conjecture about the ratio as $n \to \infty$ (cf. Problem 5).

Written Part

4. In question 2 parts (d) and (e) were similarly sized numbers, yet your algorithm probably only worked on one of them (mine did). Explain why this is. (*Hint*: try factoring $p-1$ in sage for the one that worked.) If they both worked, explain why one worked faster

5. Using your data from question 3(d), make a conjecture comparing the number of primes congruent to 1 modulo 4 and the number of primes congruent to 3 modulo 4.

6. Recall the following definition:

   Definition 1. *A composite number n is called a Carmichael Number if $a^n \equiv a \mod n$ for every integer a.*

   In essense, these are the composite numbers that satisfy Fermat's little theorem. One way you could check if a number n is a Carmichael number is to raise every integer $\leq n$ to the n'th power. But it turns out there is some interesting underlying structure to Carmichael numbers making their existence seem less coincidental. Let's explore this:

   (a) We begin by proving that our example 561 from class is a Carmichael number. Notice that $561 = 3 * 11 * 17$. Show that for every a the following congruences hold:

   $$\begin{aligned} a^{561} &\equiv a \mod 3 \\ a^{561} &\equiv a \mod 11 \\ a^{561} &\equiv a \mod 17. \end{aligned}$$

   Use this fact to prove that the same congruence holds mod 561 therefore proving that 561 is a Carmichael number.

   (b) Use the same logic to show that $75361 = 11 * 13 * 17 * 31$ is a Carmichael number.

   Hopefully we've now noticed a few patterns. Let's extrapolate these to prove some general facts about Carmichael numbers.

   (c) Show that a Carmichael number must be odd.

   (d) Show that a Carmichael number must factor into a product of distinct prime numbers (such a number is called *square free*).

   (e) Prove *Korselt's criterion*: A composite number n is a Carmichael number if and only if it is square free and for all prime divisors p of n, we have $p-1|n-1$.