CS315, Fall 2016
Homework 3
due: September 24, 2016

Problem 1: Implement an algorithm to generate prime numbers. You will need to implement the following ingredients (some of them you developed for earlier assignments):

1. A method to generate random binary numbers with n-digits (hint: no point in generating even numbersl thus, for the least significant digit there is no choice, it will have to be 1; for all other positions, generate 0 or 1 at random)
2. A method to compute modular exponentiation.
3. A method to test primality. Since the numbers you will be testing are randomly generated, use the first algorithm we discussed with a single test $3^{N-1} \equiv 1(mod\ N)$

Test your algorithm with randomly generated 16-bit numbers. Specifically, generate 100 numbers (presumably prime) using your prime-generating algorithm, and check how many of them are actually primes by a brute-force approach of trying all divisors up to the square root of the number; you will be able to use regular integer arithmetic to do it). How many times did your algorithm come back with a number that was not a prime? Should that surprise you or is it consistent with what we discussed in class?

Use your algorithm to generate prime numbers with 16, 32, 64, 128 and 256 bits. In each case, report the number of randomly generated numbers before the prime was found. What should it be in theory? Are your results consistent with the theory?

In your write up, report the 256-bit prime numbers you generated.

Finally, report CPU times taken by your algorithm to generate primes with 16, 32, 64, 128 and 256 binary digits. Based on the times, estimate the rate of growth (the degree of a polynomial that asymptotically estimates the running time). Is it consistent with the theoretical estimate of the running time of the algorithm to generate primes we derived in class. Explain.

Do not delay starting to work on that assignment. It will take you some time.

All files must be submitted as a single .zip archive. The archive must contain a file called README.txt enumerating all other files/directories in the archive, providing for each of them a brief explanation of its content. You should also include instructions explaining how to compile/run your programs. All reports, discussion, etc. must be word-processed and converted to pdf. Submit to cnavas