CSCI 2824 - Discrete Structures
Homework 5

You MUST show your work. If you only present answers you will receive minimal credit. This homework is worth 100pts.

This homework contains some problems which will require you to show work in the form of a program. You may use any language you wish. As usual using a language other than Python and C/C++ will result in extra credit.

The homework 5 submission on Moodle will allow 3 file submissions: one for .pdf, one for .tex, one for tarball with code. The tarball you submit must contain separate files for the code for each problem, that is not one file solving both problems, but each problem solved separately. Additionally you need to include a Makefile. It should contain at least two rules, one called `all:` which will compile your file if necessary (or print a message saying you don't need to compile your code) and one called `run:` which will run both of your solutions back-to-back. This way it does not matter what you call your files, or if you use third-party libraries (only use third-party libraries for Big Integers, if your language does not support them) that need command line arguments the grader does not need to know, he can simply type `$ make` and then `$ make run` and have your code compile/print a message and execute.

Due: Wednesday July 19

1. (12 points) Find the prime factorizations of the following numbers:
   (a) 209
   (b) 637
   (c) 1050703
   (d) 11!

2. (15 points) Find the greatest common divisor between the following pairs of numbers:
   (a) $13, 13^2$
   (b) $3^2 \cdot 7^3 \cdot 11, 3 \cdot 7^5 \cdot 11$
   (c) $220, 1400$

3. (4 points) The Euler ϕ-function (or totient function) is a function from $\mathbb{N} \to \mathbb{N}$ which returns the number of positive integers less than or equal to n which are relatively prime to n. E.g. $\phi(6) = 2$ since only $1, 5$ are relatively prime to 6 between 1 and 6. $\phi(8) = 4$ because $1, 3, 5, 7$ are the only values which are relatively prime between 1 and 8.
   (a) Find $\phi(10)$
   (b) Prove that n is prime if and only if $\phi(n) = n - 1$.

4. (6 points) Solve the following congruences:
   (a) $19x \equiv 4 \mod 141$
   (b) $34x \equiv 77 \mod 89$

5. (8 points) Solve the following systems for a single x (per part).
   (a) $x \equiv 2 \mod 3$, $x \equiv 1 \mod 4$, $x \equiv 3 \mod 5$
   (b) $x \equiv 1 \mod 2$, $x \equiv 2 \mod 3$, $x \equiv 3 \mod 5$, $x \equiv 4 \mod 11$.

6. (10 points) Compute the following numbers:
   (a) $11^{644} \mod 645$
   (b) $12^{2003} \mod 2037$

7. (10 points) This is a programming problem, from Project Euler. The prime factors of 13195 are 5, 7, 13 and 29. What is the largest prime factor of the number 600851475143?

   You may use any programming language to answer this (though if you use a C variant you will probably need a third party library to represent that large a number). In your .pdf write up you should place the answer with an explanation of how you got it. You should also submit your code on Moodle (along with a Makefile for any compilation).

8. (10 points) This is a programming problem, from Project Euler. By listing the first six prime numbers: 2, 3, 5, 7, 11, and 13, we can see that the 6th prime is 13. What is the 10,001st prime number?

   You may use any programming language to answer this (though if you use a C variant you will probably need a third party library to represent that large a number). In your .pdf write up you should place the answer with an explanation of how you got it. You should also submit your code on Moodle (along with a Makefile for any compilation).

9. (5 points) What sequence of pseudorandom numbers is generated using the pure multiplicative generator $x_{n+1} = 3x_n \mod 11$ with seed $x_0 = 2$?

10. (5 points) Encrypt the message WATCH YOUR STEP using the encryption function $f(p) = 3p + 7 \mod 26$, by first converting the message into numbers as discussed in class.

11. (5 points) Encrypt the message UPLOAD using the RSA encryption system as discussed in class. Use $n = 43 \cdot 59$ and $e = 13$. You may need to group letters together in different ways and pad with X's, if necessary. After encryption you may not be able to convert numbers back into letters, that is fine, however you should remember to pad the encrypted result back to a multiple of 2 digits. e.g. If the encryption of 12 is 5, you would print that as 05.

12. (10 points) In class we discussed the Diffie-Hellman Key Exchange. The method discussed in class has a vulnerability.

    Eve, an attacker, can alter messages that Alice and Bob send to each other without their knowing. To do this she intercepts (and makes some changes to) the exchanges Alice and Bob make with each other. Discover this method and describe it to me.

    Hint: You should be attacking the key-exchange. Find a method so that Alice and Eve have shared keys and Eve and Bob have shared keys (even though Alice thinks she is communicating with Bob and Bob thinks he is communicating with Alice). And remember that Eve can intercept any message Alice sends to Bob and vice versa. This means that she can stop the message from reaching its destination and send another in its place.