CPSC 418/MATH 318 Practice Problems

Euler Phi, Binary Exponentiation, Diffie-Hellman Key Agreement

1. Recall the *Euler Phi Function* defined via $\phi(m) = |\mathbb{Z}_m^*|$ for all positive integers m; that is, $\phi(m)$ is the number of integers a with $0 \leq a < m$ and $\gcd(a, m) = 1$. Compute $\phi(m)$ for the following values of m:
   (a) $m = 73$.
   (b) $m = 143$.
   (c) $m = 256$.
   (d) $m = 600$.
   (e) $m = 1$.

2. (a) Use the binary exponentiation algorithm to compute $2^{13} \pmod{15}$.
   (b) The inverse of 2 modulo 15 is easily verified to be 8, which is *not* the answer to part (a). So what is wrong with the following reasoning: "Fermat's Little Theorem gives us that $2^{14} \equiv 1 \pmod{15}$. So $2^{13} \pmod{15}$ should simply be the inverse of 2 modulo 15, which is easily computable via the extended Euclidean algorithm."

3. Suppose Alice and Bob wish to employ the Diffie-Hellman key agreement protocol to share a common secret key. They agree on the prime $p = 11$ and the base element $g = 2$.

   (a) Verify that p is a safe prime.

   (b) Verify that 2 is a primitive root of 11.

   (c) Suppose Alice chooses $a = 9$ as her secret exponent. Use the binary exponentiation algorithm to compute the element $2^9 \pmod{11}$ that Alice communicates to Bob.

   (d) Suppose Bob chooses $b = 7$ as his secret exponent. Use the binary exponentiation algorithm to compute the element $2^7 \pmod{11}$ that Bob communicates to Alice.

   (e) Perform Alice's computation of the key, i.e. use the result of part (d) and Alice's secret exponent to compute the shared key.

   (f) Perform Bob's computation of the key, i.e. use the result of part (c) and Bob's secret exponent to compute the shared key.

   Hint: The result of parts (e) and (f) should be $K = 8$.