Mathematics 243, section 3 – Algebraic Structures
Problem Set 7
due: Friday, November 9

'A' Section

1. If we are using an affine cypher and we want to include *more symbols* in our plaintext messages than just the capital letters and a blank space as in the examples we did in class, then we can do that by increasing the modulus m for the numerical form of our plain and cypher text. For this problem, say we want to include the letters $A, B, C, \ldots, Z$, the space , and the apostrophe, comma, period, and question mark. Then we can use $\mathbb{Z}_{31}$ as the numerical form of our alphabet, and make $A \leftrightarrow 0$, $B \leftrightarrow 1, \ldots, Z \leftrightarrow 25$, the space be 26, the apostrophe be 27, the comma be 28, the period be 29, and the question mark be 30.

   a. Use the affine encryption function $f(x) = 7x + 20 \pmod{31}$ to encrypt the plaintext message "Are we on for today?" Give the cyphertext in literal form (using the same alphabet).

   b. What is the decryption function $g = f^{-1}$ for this f?

   c. Use the decryption function to decrypt the cyphertext "SZQOQDUSW." (Note: the period at the end *is part of the cypher text.*)

2. Suppose an RSA public key cryptosystem has $m = 7 \cdot 11 = 77$, and an encryption exponent $e = 7$ is used. Use the 27-letter alphabet (space = 0). from our examples in class and two-digit blocks.

   a. Encrypt the plaintext message "GO FOR IT" using this system (Note: the cyphertext will be in numerical, not literal form.)

   b. What is the ("secret") decryption exponent d for this system?

   c. Use it to decrypt the cyphertext: "42, 71, 23, 1, 53, 10, 71, 68, 47" (Why didn't I actually include spaces between the words here?)

'B' Section

The Euler ϕ-function (or totient) is defined for $n > 0$ in $\mathbb{Z}$ by $\phi(n)$ = the number of classes $[a]$ in $\mathbb{Z}_n$ for which a multiplicative inverse exists in $\mathbb{Z}_n$ (this is the same as the number of a with $0 \le a < n$ and $\gcd(a, n) = 1$).

1. Find $\phi(11)$, $\phi(16)$, and $\phi(20)$.

2. Prove that the number of ordered pairs (a, b) for which $f(x) = ax + b \pmod{n}$ defines an invertible affine encryption function on $\mathbb{Z}_n$ is $n \cdot \phi(n)$.

3. Show that the set of affine encryption functions is closed under composition.

4. If $n = pq$ where p, q are distinct primes, prove that $\phi(n) = (p-1)(q-1)$.
5. If $n = p^e$ where p is prime and $e \geq 1$, then show $\phi(n) = p^e - p^{e-1} = p^{e-1}(p-1)$.