Math 116
Homework 1
Due Thursday, January 14, 2016

Please read Chapter 1 in the textbook.

1. For each of the following, find the unique integer between 0 and $n-1$ that is equivalent to the expression given (where n is the modulus in the expression). Do these by hand, without a computer.

   (a) $543 \cdot 379 \pmod{12}$

   (b) $29513 \cdot 93723208 \pmod{100}$

   (c) $24637^3 \pmod{15}$

   (d) $82375^{5628} \pmod{18}$ *(Hint: What is* $82375^3 \pmod{18}$*?)*

   (e) $46249^{601} \pmod{18}$ *(Hint: What is* $46249^3 \pmod{18}$*?)*

2. Alice has announced that anyone who wants to send her encrypted ASCII messages should take each character (a number between 0 and 127) and multiply it by 69 (mod 128). Bob sends Alice the following ciphertext:

   $$84,\ 107,\ 38,\ 3,\ 68,\ 32,\ 68,\ 58,\ 9,\ 127,\ 68,\ 32,\ 25,\ 78,\ 57$$

   (a) Find a number d such that $69 \cdot d \equiv 1 \pmod{128}$. (If you want, you can do this by a quick brute force computer search, since the numbers are small. We'll learn a much better way soon.)

   (b) Use your answer to part (a) to decrypt Bob's message. (You can get back to his original text by looking up an ASCII table online. Or just use a computer.)

3. Let n be an integer. Recall that in class we made the following definition: for any $a, b \in \mathbb{Z}$, we say $a \equiv b \pmod{n}$ if (and only if) $n \mid (a-b)$, or in other words, if $a - b = nk$ for some $k \in \mathbb{Z}$. Prove that this is an equivalence relation on $\mathbb{Z}$. That is, prove this relation is

   (a) **reflexive:** for all $a \in \mathbb{Z}$, $a \equiv a \pmod{n}$;

   (b) **symmetric:** for all $a, b \in \mathbb{Z}$, if $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$;

   (c) and **transitive:** for all $a, b, c \in \mathbb{Z}$, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

4. Let n be an integer. In class we stated that addition, subtraction, and multiplication are well defined modulo n, and we proved the claims about addition and multiplication.

Prove the remaining claim about subtraction. That is, prove that if $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

$$a - b \equiv a' - b' \pmod{n}.$$

5. Intuitively, we think of decryption as the inverse of encryption. However, strictly speaking, the mathematical definition of encryption and decryption functions given in class did not require these functions to be inverses. Using the notation $E_k \colon \mathcal{P} \to \mathcal{C}$ and $D_k \colon \mathcal{C} \to \mathcal{P}$, we simply require that

$$D_k(E_k(m)) = m \text{ for all } m \in \mathcal{P}, \tag{1}$$

or in other words, that $D_k \circ E_k = 1_{\mathcal{P}}$ (the identity function on $\mathcal{P}$). Mathematically, in order for D_k to be the inverse of E_k, we would need to also require that

$$E_k(D_k(m)) = m \text{ for all } m \in \mathcal{C}, \tag{2}$$

or in other words, that $E_k \circ D_k = 1_{\mathcal{C}}$. Practically speaking, equation (2) is usually not as important as (1), because it's about starting with a ciphertext message m, and decrypting it and then re-encrypting it with the same key. However there are cases where (2) is desirable. We saw one application in class on Monday: if an asymmetric cipher has this property, then it can be used not only for encryption, but also for *digital signatures*.

   (a) Give an example of two sets X and Y and a pair of functions $e \colon X \to Y$ and $d \colon Y \to X$ for which $d(e(x)) = x$ for all $x \in X$, but there is some $y \in Y$ for which $e(d(y)) \neq y$. (In other words, $d \circ e = 1_X$ but $e \circ d \neq 1_Y$.)

   (b) Now suppose that X and Y are *finite sets* containing the *same number* of elements, and $f \colon X \to Y$ is a function. Prove that if f is one-to-one, then f is onto. *(Hint: The pigeonhole principle.)*
   (Note that the converse of this is also true, but it's trickier to prove. If you want, see if you can prove it: if f is onto, then f is one-to-one.)

   (c) Use part (b) to prove that if the plaintext space $\mathcal{P}$ and the ciphertext space $\mathcal{C}$ are finite sets of the same size, then the decryption function D_k really is the inverse of the encryption function E_k. That is, in this case, assuming (1) automatically implies that (2) is true.

The hypothesis of part (c) is true for many ciphers in the real world, both symmetric and asymmetric.