Math 455.1 **Homework Set 5** **Spring, 2009**

Due: Wednesday, April 8 – *postponed* (start of class)

- Work ***individually***, that is, *not* in a team. See the About > Homework sets page on the Math 455 web site regarding collaboration and plagiarism.
- For *Mathematica* work here, turn in printed pages. Try to place associated written work directly onto such printed pages (or include text cells there).
- For affine ciphers, be sure to follow the convention of first adding and then multiplying. And use the convention that `A` is coded numerically as 0, `B` is coded as 1, etc. Also, work with the numerical equivalents of the text letters and not the letters themselves. See notebook `AffineEncrypt.nb`.

1. (a) Use the *definition* of congruence (in terms of divisibility) to prove the following for all integers a, b, c and all integers $m > 1$: If $c+a \equiv c+b \pmod{m}$, then $a \equiv b \pmod{m}$.

   (b) Is the analog of (a) for multiplication, instead of addition, also true? If so, prove it (in general); if not, give a counterexample.

2. Use an affine cipher with additive key 23 and multiplicative key 5 to encrypt the plaintext:

   ```
   Government is, or ought to be, instituted for the common benefit,
   protection, and security, of the people, nation, or community.
   ```

   For your convenience, this text is available in the notebook `Set5#2.nb`. You must first strip out all spaces and punctuation, convert all letters to upper-case, and encode into integers; then encrypt into integers and decode the result into ciphertext split into groups of 5 letters. You may use *Mathematica* for some or all of the work.

3. Use notebook `Set5#3.nb` to obtain your own, individual ciphertext. That ciphertext was obtained by using either a multiplicative cipher or an additive cipher. Break the cipher and decrypt the ciphertext.

   The ciphertext is short, so you may or may not be able to exploit letter frequencies. Try up to the three most likely possibilities for the most frequent letter in the ciphertext (and include the results from those trials). If you cannot succeed after three trials—and *only* in that case—apply "brute force", that is, try all possibilities. See notebook `BreakAffineCipher.nb` for examples of breaking such ciphers.

4. Alice uses the affine encryption system with key $(4, 3)$—that is, multiplicative key 4 and additive key 3—to send you the ciphertext message `SCCEGOMME`. She tells you she is using this system with this key.

   (a) Try to decrypt (into plaintext letters, eventually) the numerical form of the ciphertext. You should find that you cannot do so unambiguously. So determine at least four of the possibilities for the plaintext message that Alice sent. (Do *not* rely upon the meaning of the message—Alice could have sent nonsense words!)

(b) What is it about the key for this affine system that prevents you from unambiguously decrypting the ciphtertext?

5. Use the addition table for $\mathbb{Z}_6$ to find the additive inverse of each element of $\mathbb{Z}_6$. (In Z_m, an *additive inverse* of $[a]$ is an element $[b]$ for which $[a] + [b] = [0]$.)

6. (a) Without the computer, construct the *multiplication* table for $\mathbb{Z}_6$.

   (b) Use *Mathematica* to construct the multiplication table for $\mathbb{Z}_7$. Use as table entries actual integers $0, 1, 2, \ldots, 6$ rather than their congruence classes. First define a function `times7` of two arguments that implements multiplication modulo 7; for example, `times7[2, 5]` should have result `3`. Then use *Mathematica*'s function `Outer` to construct the multiplication table. Format the result as a table! (For partial credit, do it without *Mathematica*.)

7. (a) How you can tell just by looking at the multiplication table of $\mathbb{Z}_m$ whether *every* nonzero element of $\mathbb{Z}_m$ has a multiplicative inverse? Arrive at your answer by examining the multiplication tables of $\mathbb{Z}_6$, $\mathbb{Z}_7$, and such other $\mathbb{Z}_m$ as you find necessary.

   (b) Which moduli m seem to have the property that every nonzero element of $\mathbb{Z}_m$ has a multiplicative inverse? To arrive at your answer, gather the evidence from the multiplication tables and by applying your answer to (a).

   At this point, you are *not* being asked to give any mathematical proof: you are just making a conjecture based upon some evidence.