Math 25 — Assignment 4

Due Thursday, October 27th, *beginning of class*.

1. You'll want a calculator for this exercise. Let $(e, n) = (17, 397801)$. What is the ciphertext (encrypted message) associated to

   BOB LOBLAW LAW BLOG

   In this case, we associate spaces to the value 32, pad with zeros, and use chunks of 3 characters. For example, we get the encoding

   $$\texttt{'EX T'} \to (052432 \pmod n,\ 200000 \pmod n).$$

   Solution: First we carve the string into chunks, giving

   'BOB' | ' LO' | 'BLA' | 'W L' | 'AW ' | 'BLO' | 'G'

   Converting to numbers gives

   $$021502 \mid 321215 \mid 021201 \mid 233212 \mid 012332 \mid 021215 \mid 070000$$

   To encrypt each block m, we simply compute $m^e \pmod n$. This gives the ciphertext:

   $$004050 \mid 348060 \mid 334015 \mid 175890 \mid 329235 \mid 115807 \mid 026644$$

   Remark: Adding leading zeros is nice, since chunks always have a fixed size. The ciphertext really looks like

   $$004050348060334015175890329235115807026644$$

   and the decrypted encoded text looks like

   $$021502321215021201233212012332021215070000$$

   Knowing the chunks have six symbols makes parsing easier. (For a computer.)

   Remark: Python makes the conversion easy.

   ```
   >>> [ord(c)-64 for c in 'BOB LOBLAW LAW BLOG']
   [2, 15, 2, -32, 12, 15, 2, 12, 1, 23, -32, 12, 1, 23, -32, 2, 12, 15, 7]
   ```

   Remark: In practice, characters are encoded/decoded via their ASCII or Unicode values.

2. Let a, n be coprime integers and let e be coprime to $\phi(n)$. If a has order d in $\mathbb{Z}/n\mathbb{Z}^\times$, prove that a^e also has order d.

   Solution: Because e is coprime to $\phi(n)$, it is coprime to any divisor of $\phi(n)$. By Lagrange's theorem, the order d of the element a must be a divisor of $\phi(n)$. In particular, there exists an x such that $ex \equiv 1 \pmod d$. Now

   $$a \equiv (a^e)^x \pmod n.$$

   If m is the order of a^e, then $a^m \equiv a^{exm} \equiv 1 \pmod n$. In particular, $d \mid m$. On the other hand,

   $$(a^e)^d \equiv (a^d)^e \equiv 1 \pmod n,$$

   so $m \mid d$. Thus $d = m$.