MATH 310: FRIDAY MARCH 21

(1) Do all of exercises from 5.4. These are going to be **very** impotant when we talk about quadratic reciprocity later. Here are some comments:
   1. We did the first two in class the last day. The third is much the same. Practice especially things like writing $x^4 \mod 7$ when $x = 6$ not as 6^4 but as $(-1)^4$ modulo 7.
   2. Recall that $k!$ divides the product of *any* k consectuve integers.
   3. My hint on this was off the last day: Replace the terms x and h respectively in the Taylor series $f(x + h)$ with the terms m and rp^s respectively.
   4. A nice extension of **3.**
   5. A lovely application of **4.**. Note that $343 = 7^3$.
   6. By $x^4 + 1$ being irreducible over the integers means that $x^4 + 1$ does not factor into linear factors. However, in $\mod 2$ $x^4 + 1 = (x + 1)^4$. Can you look at the other modulo systems sugested here.
   7. Note that $1, 2, \ldots, p - 1$ is a reduced reside system mod p. Hmmmm...
   8. Oh my! Look at that!

(2) Last day we finished with Theorem 7-2, a gem that stated that if a belongs to h modulo m and of $a^r \equiv 1 \mod m$ then $h \mid r$. In particular, h divides $\phi(m)$, as we saw with the example of 3 belonging to 5 modulo 11 and how $5 \mid \phi(11)$. This brings us to the new reading for today: Definition 7-2 defined an integer g to be a *primitive root* modulo m if g belongs to $\phi(m)$. Theorem 7-3 is the very reasonable statement that the first $\phi(m)$ positive powers of such a g form a reduced residue system. Example 7-2 then shows that there are m's that have no primitive roots.

   Theorem 7-4 is the tiniest bit technical to state so to convince you that it is worth understanding it, consider its corollary, 7-1 which is the rather delightful statement that if you have one primitive root modulo m then you can generate a bunch of others as powers of that primitive root, in particular, those powers that are relatively prime to $\phi(m)$. Furthermore, Theorem 7-5 tells us that if there is one primitive root modulo m then there must be precisely $\phi(\phi(m))$ of them.

   Do all exercises from 7-1

   1.–5. This is a nice collection of exercises that generalises the log of a number, but modulo m.
   6. This will be a good exercise upon which to confirm all the theorems and corollaries of the section.

(3) Lastly, read the first paragraph pf Section 7-2, where it describes the m's that have a primitive root. What are the ten smallest m's which **do not** have primitive roots?