Worksheet 11

Problems marked with a $(*)$ are "key results".

0. If you didn't already, go attempt problem 4 from Friday's worksheet.

1. Suppose that $m, n > 1$ are relatively prime integers. Find a solution to the system of congruences $x \equiv 1 \bmod m$ and $x \equiv 0 \bmod n$.

2. (a) $(*)$ Now suppose that a, b are arbitrary integers and $m, n > 1$ are relatively prime. Find a solution to the system of congruences $x \equiv a \bmod m$ and $x \equiv b \bmod n$.

   (b) $(*)$ Prove that any solution to the system is unique mod mn. That is, if c, c' are integers that solve the system of congruences, then $c \equiv c' \bmod mn$.

   Combing the two parts, you get the following result: when $(m, n) = 1$ there is a unique solution mod mn to the system of congruences $x \equiv a \bmod m$ and $x \equiv b \bmod n$.

3. (a) Solve the system of congruences $x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 5$, $x \equiv 2 \bmod 7$. (This problem was first solved by ancient Chinese mathematican Sun-tzu in the 3rd century. Unrelated to the war general!)

   (b) Show that there is no solution to the system $x \equiv 1 \bmod 6$, $x \equiv 4 \bmod 10$, $x \equiv 7 \bmod 15$.

   (c) What went wrong in the second example? Conjecture a condition on the moduli for when a system of 3 congruences will have a solution. Do you think your condition will work for more than 3 moduli?

4. Define a function φ by $\varphi(n) = \#\{1 \leq a \leq n : (a, n) = 1\}$, the number of integers between 1 and n that are co-prime to n. For example, $\varphi(6) = 2$, because the integers between 1 and 6 that are co-prime to 6 are $1, 5$.

   (a) $\varphi(n)$ counts the number a certain type of element in $\mathbb{Z}/n\mathbb{Z}$. What is it counting?

   (b) Compute $\varphi(p)$ when p is prime.

   (c) $(*)$ Compute $\varphi(p^k)$ for $k \geq 1$.

5. Create a table of the values of $\varphi(n)$ for n up until 30. What patterns do you notice? Come up with some conjectures!