Worksheet 10

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

0. Finish any of the worksheet problems $1-3$ from last time that you didn't get to – they're all important!

1. (a) $(*)$ Prove that $ax \equiv 1 \bmod n$ is solvable if and only if $\gcd(a, n) = 1$. This says that $a \in \mathbb{Z}/n\mathbb{Z}$ is invertible if and only if $\gcd(a, n) = 1$.
   (b) Knowing that $2^{-1} \equiv 7 \bmod 13$, how could you solve the congruence $2x \equiv 11 \bmod 13$?
   (c) Describe an algorithm for computing the inverse of $a \bmod n$. *(Hint: this is a very familiar computation by this point!)*
   (d) Is the congruence $24x \equiv 57 \bmod 215$ solvable? If so, find the solution. If not, explain why.

2. When p is a prime, $\mathbb{Z}/p\mathbb{Z}$ has a nicer structure than $\mathbb{Z}/n\mathbb{Z}$ for composite n.
   (a) $(*)$ Prove the *cancellation law*, that if $ab \equiv ac \bmod n$ and $\gcd(a, n) = 1$, that $b \equiv c \bmod n$. (In particular, this shows that cancellation always works mod p).
   (b) $(*)$ On the last worksheet, you saw that in general, $x^2 = 1$ may have more than two solutions in $\mathbb{Z}/n\mathbb{Z}$ and you can possibly have $ab = 0$ with $a, b \neq 0$ in $\mathbb{Z}/n\mathbb{Z}$. Prove that when n is *prime*, this cannot happen. That is, prove that if $x^2 \equiv 1 \bmod p$ then $x \equiv \pm 1 \bmod p$ and if $ab \equiv 0 \bmod p$ then $a \equiv 0 \bmod p$ or $b \equiv 0 \bmod p$.

3. On homework 2, you proved that for any odd integer $n > 1$, that $8 \mid n^2 - 1$. Give a new proof of this fact using modular arithmetic.

4. Find an integer x such that $x \equiv 1 \bmod 3$ and $x \equiv 2 \bmod 4$. How many more solutions can you find?

5. (a) Make a table of all the powers of 2 in $\mathbb{Z}/13\mathbb{Z}$ (use WolframAlpha for the computation if you wish). What do you notice?
   (b) Using your table, solve $x^2 = 10$ and $x^3 = 5$ in $\mathbb{Z}/13\mathbb{Z}$.