Math 458
Homework Due Wednesday, April 24

1. Do the following problems from the textbook:

   2.17a, 2.18ad, 2.19, 2.23ac, 2.28a

2. Using only a hand-held caluclator and half a sheet of paper (and a pen or pencil), find the remainder when $5^{1242101}$ is divided by 149. (Hint: 149 is prime. Use a combination of Fermat's Little Theorem and the fast powering algorithm).

3. In class (and in the textbook) we learned that a list of N numbers could be sorted from least to greatest in $\mathcal{O}(N \log N)$ steps. This problem will show you how to do this.

   (a) Suppose given $a_1 \leq a_2 \leq \ldots \leq a_n$ and another number x. Give an algorithm for placing x into the list (in the correct spot with respect to $\leq$) that takes at most $\lfloor \log_2(n) \rfloor + 1$ steps. (By a "step" I mean one $\leq$ comparison. For instance, the "brute force" algorithm would compare x to a_1, then if x is bigger compare x to a_2, and so on...and this would take at most n steps). [Warning: A complete explanation for the number of steps is a bit tricky, so it is enough for me if you just demonstrate with some examples.]

   (b) Let $N = 2^k$. Here is an algorithm for sorting a list of N elements. If $N = 2$, do one comparison and sort the two elements in the evident way. If $N > 2$, first sort the first $N/2$ elements by recursion: this will give you $a_1 \leq a_2 \leq \cdots \leq a_{N/2}$. For each of the remaining $N/2$ elements, place them one by one into the a_i list using the algorithm from part (a).

   Let $p(k)$ be the maximum number of steps needed to complete the above algorithm. Explain why
   $$p(k) \leq p(k-1) + 2^{k-1} \cdot k$$
   for all k.

   (c) Continuing with notation as in part (b), explain why
   $$p(k) \leq 1 + 2^2 \cdot 3 + 2^3 \cdot 4 + 2^4 \cdot 5 + \cdots + 2^{k-1} \cdot k \leq 2^k \cdot k.$$

   (d) Complete the explanation of why the algorithm takes $\mathcal{O}(N \log N)$ steps, at least when $N = 2^k$.

4. Explain why the equation $x^2 = 1$ has four solutions in $\mathbb{Z}/(pq)$ when p and q are distinct odd primes. (Use the Chinese Remainder Theorem).

5. Let us say that $\mathbb{Z}/m$ has property (P) if every unit a in $\mathbb{Z}/m$ satisfies $a^2 = 1$. In other words, property (P) says that every unit is a square root ot 1.
   (a) For each $m \in \{2, 3, \ldots, 10\}$, determine if $\mathbb{Z}/m$ has property (P). In each case, explain how you know that it does or does not.
   (b) Suppose that $m > 1$ is an odd number such that $\mathbb{Z}/m$ has property (P). Using that 2 is a unit in $\mathbb{Z}/m$, prove that $m = 3$.
   (c) If $m = 2^k$ and $\mathbb{Z}/m$ has property (P), prove that $k \leq 3$. (Hint: Find a small unit that you know.)

Note: On the next homework you will determine *all* numbers m such that $\mathbb{Z}/m$ has property (P). Oooh, the suspense.

6. (Extra Credit Challenge Question) 2.25b from the book. I don't know how to do this, but I'm interested in finding out.