Homework 2

Due Friday, February 5

Practice Problems

You don't need to turn in solutions to the following textbook problems, but you should try all of them.

- Section 1.3: 7, 17, 20, 34
- Section 2.1: 3, 5, 6, 13, 21
- Section 2.2: 2, 4, 13, 14, 15
- Extra problem: Without using a calculator, prove that $1782^{12} + 1841^{12} = 1922^{12}$ is false.[1]

Problems to turn in

1. Let $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ and $b = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ be the prime factorizations of a and b. (That is, $p_1, p_2, \ldots, p_k$ are distinct primes and each $r_i, s_i \geq 0$.) Prove that $a \mid b$ if and only if $r_i \leq s_i$ for every i.

2. Suppose $a, b \in \mathbb{Z}$, and let n be a positive integer. Prove that $a \mid b$ if and only if $a^n \mid b^n$.

3. Suppose a and n are positive integers. Prove that $\sqrt[n]{a}$ is either an integer or an irrational number.

   Note: This makes it easy to determine whether $\sqrt[n]{a}$ is irrational; if it's not an integer, then it must be irrational. For example, $\sqrt[4]{120}$ is clearly not an integer, so we know that it is irrational.

Recall that the binomial coefficients are defined by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

where n is a non-negative integer and $k \in \{0, 1, \ldots, n\}$. These numbers are called binomial coefficients because they are the coefficients when you expand a power of a binomial:

$$(x+y)^n = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

For this assignment, you may assume the above theorem without proof. Since it is obvious that the coefficients of $(x+y)^n$ are integers, you may therefore also assume that the binomial coefficients are all integers.

[1] This equation was seen in the Simpsons episode "Treehouse of Horror VI." If it were true, it would be a counterexample to Fermat's Last Theorem.

4. Prove that if p is prime and $1 \leq k \leq p-1$, then $p \mid \binom{p}{k}$.

5. Prove that if p is prime, then for any $a, b \in \mathbb{Z}$,

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

   Note: This is not necessarily true if p is composite. For example, $(1+1)^4 \not\equiv 1^4 + 1^4 \pmod{4}$.

6. Find all solutions to $X^3 = 3$ in $\mathbb{Z}/5\mathbb{Z}$. (Be sure to prove that you found all the solutions.)