|||||

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.

   Solution:

   We do an extra side proof: If $a = mn$ for $m, n \in \mathbb{Z}$ and $a \mid b$, then $m \mid b$. Clearly, if $a \mid b$, then $b = ak$ for $k \in \mathbb{Z}$. Then $b = (mn)k = (nk)m$. Since nk, $m \mid b$.

   i) Going back to our proof, suppose $a \mid b$ then $p_1^{r_1}p_2^{r_2}...p_k^{r_k} \mid p_1^{s_1}p_2^{s_2}...p_k^{s_k}$. Without loss of generality, take $m = p_1^{r_1}$. By the statement proven above, $p_1^{r_1} \mid p_1^{s_1}p_2^{s_2}...p_k^{s_k}$.

   We have $p_1, p_2, ...p_k$ are distinct primes, $(p_1, p_2) = (p_1, p_3) = ... = (p_1, p_k) = 1$. Now, we use the statement proven from problem 5, HW1: "If $a, b, c \in \mathbb{Z}$and $(a, c) = (b, c) = 1$, then $(ab, c) = 1$". Since $(p_1, p_2) = 1$ with $c = p_1$, then $(p_1, p_2^{s_2}) = 1$. Similarly with $c = p_2^{s_2}$, we get $(p_1^{s_1}, p_2^{s_2}) = 1$.

   Hence $(p_1^{s_1}, p_i^{s_i}) = 1$ for $i = 2, 3, ..., k$.

   We once again can use the statement recursively and get $(p_1^{s_1}, p_2^{s_2}) = (p_1^{s_1}, p_2^{s_2}p_3^{s_3}) = (p_1^{s_1}, p_2^{s_2}p_3^{s_3}...p_k^{s_k}) = 1$.

   Now, $p_1^{r_1} \mid p_1^{s_1}p_2^{s_2}...p_k^{s_k}$, and $(p_1^{s_1}, p_2^{s_2}p_3^{s_3}...p_k^{s_k}) = 1$. By the theorem: "If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$",we can conclude $p_1^{r_1} \mid p_1^{s_1}$.

   Hence $p_1^{r_1}$ is a divisor of $p_1^{s_1}$, which implies $|p_1^{r_1}| \leq |p_1^{s_1}|$ or $r_1 \leq s_1$.

   ii) Conversely, it is clear that $r_1 \leq s_1$, then $r_1 + m_1 = s_1$ for $m_1 \in \mathbb{Z}, m \geq 0$.

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

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.)