**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, $p_1^{r_1} \mid p_1^{s_1} p_2^{s_2} ... p_k^{s_k}$.

   Since $p_1, p_2, ...p_k$ 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 $|\mathrm{p}_1^{r_1}| \leq |p_1^{s_1}|$ 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 $m_1 \in \mathbb{Z}, m \geq 0$. Then $p_1^{r_1} \mid p_1^{r_1} p_1^{m_1} = p_1^{r_1 + m_1} = p_1^{s_1}$

   Apply this for $i = 1, 2..., k$, we get $p_1^{r_1} p_2^{r_2} ... p_k^{r_k} \mid p_1^{s_1} p_2^{s_2} ... p_k^{s_k}$, which proves $a \mid b$.

   Therefore, from i) and ii), $a \mid b$ if and only if $r_i \leq s_i$ for every $i$. □

[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.

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

   **Solution:** We do an extra side proof: If $u \mid m$ and $v \mid n$ with $u, v, m, n \in \mathbb{Z}$, then $uv \mid mn$. Clearly, $u \mid m$ and $v \mid n$ implies $m = uq$ and $n = vp$for $p, q \in \mathbb{Z}$. Hence $mn = (pq)uv$ or $uv \mid mn$.

   Going back to our proof. Suppose $a \mid b$, apply this recursively with $a \mid b$, we get $a^n \mid b^n$.

   Conversely, suppose $a^n \mid b^n$. 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 $b$, $p_1, p_2, \ldots, p_k$ are distinct, and each $r_i, s_i \geq 0$. Using result of 1), since $a^n \mid b^n$ and $n$ is a positive integer, $nr_i \leq ns_i$ or $r_i \leq s_i$. This, by result of 1), implies $a \mid b$.

   Therefore, $a \mid b$ 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.

   **Solution:** Suppose $a$ and $n$ are positive integers. If $\sqrt[n]{a}$ is an integer, we are done. If $\sqrt[n]{a}$ is not an integer and is rational, then there exist $p, q \in \mathbb{Z}, q \neq 0$, $(p, q) = 1$ such that $\sqrt[n]{a} = \frac{p}{q}$. Then $a = \frac{p^n}{q^n}$ or $aq^n = p^n$ which implies $q^n \mid p^n$. Using result of 2), we get $q \mid p$ (Contradicts $(p, q) = 1$!).

   Thus, if $a$ and $n$ are positive integers, $\sqrt[n]{a}$ is either an integer or an irrational number. □

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:

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

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.

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

   **Solution:** We have

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = p.\frac{(p-1)!}{k!(p-k)!},$$

   .

   If $\frac{(p-1)!}{k!(p-k)!}$ is an integer, we get $p \mid \binom{p}{k}$.

If $\frac{(p-1)!}{k!(p-k)!}$is not an integer, since its numerator and denominator are products of integers, $\frac{(p-1)!}{k!(p-k)!}$ is rational. Let $\frac{(p-1)!}{k!(p-k)!}=\frac{a}{b}$ for $a, b \in \mathbb{Z}, (a,b)=1, b \neq 0$. Now $\binom{p}{k}=p.\frac{a}{b}$ or $\binom{p}{k}.b=pa$. This implies $p \mid \binom{p}{k}b$. By theorem in class, with $p$ prime, $p \mid \binom{p}{k}$ or $p \mid b$. If $p \mid \binom{p}{k}$, we are done. For $p \mid b$, this cannot happen, since $1 \leq k \leq p-1$ and $p$ prime, $p \nmid k!$ and $p \nmid (p-k)!$ or $p \nmid k!(p-k)!$ meaning $p \nmid b$.

Therefore, 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, $(1+1)^4 \not\equiv 1^4 + 1^4 \pmod{4}$.

**Solution:** Using the binomial expansion formula

$$(a+b)^p = \binom{p}{0}a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + \binom{p}{p}b^n$$

From 4), we can conclude all $\binom{p}{k}$ with $n$ prime and $1 \leq k \leq p-1$ satisfies $p \mid \binom{p}{k}$. Hence

$$\begin{aligned}(a+b)^p &\equiv \binom{p}{0}a^p + \binom{p}{p}b^p \pmod{p} \\ &\equiv a^p + b^p \pmod{p}. \quad \square\end{aligned}$$

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

**Solution:** For $X \in \mathbb{Z}/5\mathbb{Z}$, there are only five possible values of $X$,
If $X=0$, $X^3 = 0 \neq 3$, so $X=0$ is NOT a solution.
If $X=1$, $X^3 = 1 \neq 3$, so $X=1$ is NOT a solution.
If $X=2$, $X^3 = 8 = 3$, so $X=2$ is a solution.
If $X=3$, $X^3 = 27 = 2 \neq 3$, so $X=3$ is NOT a solution.
If $X=4$, $X^3 = 64 = 4 \neq 3$, so $X=4$ is NOT a solution.

In summary, $X=2$ is the only solution of $X^3=3$ in $\mathbb{Z}/5\mathbb{Z}$. □