Steven Rosendahl
Homework 4

1. If p is prime and $p \mid a^k$, prove that $p \mid a$. Conclude that $p^k \mid a^k$.

   Since $p \mid a^k$, we have that $p \mid aa^{k-1}$. Then $p \mid a$ or $p \mid a^{k-1}$, but not both. If we assume that $p \mid a^{k-1}$, we can say that $p \mid aa^{k-2}$. If $p \mid a^{k-2}$, then we have that $p \mid aa^{k-3}$. If we repeat this process, we will ultimately have that $p \mid aa^0$. Then $p \mid a$ or $p \mid a^0$. If $p \mid a$, then we are done. If $p \mid a^0$, then $p \mid 1$, which is a contradiction. Therefore, p must divide a.

   Assume $p \mid a$. Then $a = pm$ for some $m \in \mathbb{Z}$. Raising both sides to the k power gives $a^k = p^k m^k$. Since $m^k \in \mathbb{Z}$, we can say that $m^k = j$. Then $a^k = p^k j$, so $p^k \mid a^k$.

   $\triangle$

2. Suppose that a and b are positive integers.

   (a) If $a^2 \mid b^2$ prove that $a \mid b$. (Hint: Assuming that $a^2 m = b^2$, use unique factorization to prove that m is a perfect square.)

   Assume that $a^2 \mid b^2$. Then $b^2 = a^2 m$ for some $m \in \mathbb{Z}$. By the Fundamental Theorem of Arithmetic, we have that $(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_j^{\alpha_j})^2 = (p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k})^2 m$ for $j, k \in \mathbb{Z}$ and $\alpha, \beta \in \mathbb{N}$. Then we can say that

   $$\frac{(p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k})^2}{(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_j^{\alpha_j})^2} = m \in \mathbb{Z}.$$

   Therefore, m is a perfect square, so we can take its square root. Let $n = \sqrt{m}$. Then $\sqrt{a^2 m} = \sqrt{b^2}$, or $an = b$, so $a|b$.

   (b) If n is a positive integer such that $a^n \mid b^n$ can we conclude that $a \mid b$? Either prove your answer or provide a counterexample.

   By the same argument used above, we can say

   $$\frac{b^n}{a^n} = \frac{(p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k})^n}{(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_j^{\alpha_j})^n} = m \in \mathbb{Z}.$$

   Therefore, m is a perfect n^{th} power, so we can say $j = \sqrt[n]{m}$. Then $\sqrt[n]{b^n} = \sqrt[n]{a^n m}$ simplifies to $b = aj$. Therefore, $a|b$.

   $\triangle$

3. Suppose that a and b are positive integers and $p_1, p_2, \dots, p_n$ are primes such that

   $$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \qquad \text{and} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n},$$

   where α_i and β_i are non-negative (possibly equal to 0) integers. Prove that

   $$lcm(a,b) = p_1^{max(\alpha_1,\beta_1)} p_2^{max(\alpha_2,\beta_2)} \dots p_n^{max(\alpha_n,\beta_n)}.$$

   Let $L = lcm(a,b)$. We have by definition that $a \mid L$ and $b \mid L$. If we consider the case where $a \mid L$, then we have that $L = am$ for some $m \in \mathbb{Z}$. We can arrange this as $\frac{L}{a}$, which is

   $$\frac{L}{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}} = \frac{p_1^{\gamma_1} p_2^{\gamma_2} \dots p_n^{\gamma_n}}{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}} \text{ by the FTA.}$$

   If we assume that $\gamma_i < \alpha_i$ for some $i \leq n$, then $L < a$, and $\frac{L}{a} \notin \mathbb{Z}$, which is a contradiction; we must have that $\gamma_i \geq \alpha_i$. Similarly, we can express $b \mid L$ as

   $$\frac{p_1^{\gamma_1} p_2^{\gamma_2} \dots p_n^{\gamma_n}}{p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}} = q \in \mathbb{Z}.$$

By the same argument, we must have that we must have that $\gamma_i \geq \beta_i$. If we take any arbitrary α_i such that $\alpha_i < \beta_i$, then letting $\gamma_i = \alpha_i$ would cause $\frac{L}{b} \notin \mathbb{Z}$; we also have that taking $\gamma_i = \beta_i$ when $\beta_i < \alpha_i$ will cause $\frac{L}{a} \notin \mathbb{Z}$. Therefore, γ_i must be the maximum of α_i, β_i for all i. We can conclude that the prime factorization of L must be $p_1^{max(\alpha_1,\beta_1)} p_2^{max(\alpha_2,\beta_2)} \ldots p_n^{max(\alpha_n,\beta_n)}$.

$\triangle$

4. Determine whether each of the following statements is true or false. If true, prove it. If false, provide a counterexample.

   (a) If $gcd(a, p^2) = p$ then $gcd(a^2, p^2) = p^2$.

   We know that $p \mid a$ by the definition of the gcd. We can say that $a = pn$ for some $n \in \mathbb{Z}$. Then $a^2 = p^2n^2$, so $p^2 \mid a^2$. Since p^2 is the greatest thing that divides p^2 and $a > p$ so $a^2 > p^2$, $gcd(a^2, p^2) = p^2$.

   (b) If $gcd(a, p^2) = p$ and $gcd(b, p^2) = p^2$ then $gcd(ab, p^4) = p^3$.

   If we take the case where $a = p$ and $b = p^3$, then we have $gcd(p, p^2) = p$ and $gcd(p^3, p^2) = p^2$. However, $gcd(p^4, p^4) \neq p^3$.

   (c) If $gcd(a, p^2) = p$ then $gcd(a + p, p^2) = p$.

   If we take $a, p = 2$, then we have that $gcd(2, 4) = 2$, but $gcd(4, 4) \neq 2$.

5. Prove that every prime $p \neq 3$ has the form $3q + 1$ or $3q + 2$ for some integer q. Moreover, prove that there are infinitely many primes of the form $3q + 2$.

   If we consider a prime number $p \neq 3$, we will get a remainder of either 1 or 2 when we divide it by three; if we get a remainder of 0, then that number was a multiple of 3 and therefore not prime. We also know that all prime numbers above 3 are odd. Therefore, by the division algorithm, we have that $p = 3q + 1$ or $p = 3q + 2$.

   Assume that there are finitely many primes of the form $3q + 2$. Then we can say

$$
\begin{aligned}
p_1 &= 3q_1 + 2 \\
p_2 &= 3q_2 + 2 \\
&\ldots \\
p_n &= 3q_n + 2
\end{aligned}
$$

   We will let $m = 3p_1p_2 \ldots p_k - 1$, which we can express as $3p_1p_2 \ldots p_k - 3 + 2$. By factoring we have that $m = 3(p_1p_2 \ldots p_k - 1) + 2$. Then we have a prime $p = 3q + 2$ that divides m. Since there are finitely many primes of this form, we have that $p = p_i$ for some $i \leq n$. Without loss of generality, we will let $i = 1$. Then we have

$$
\begin{aligned}
1 &= 3(p_1p_2 \ldots p_n) - m \\
&= p_1(3p_2p_3 \ldots p_n - \frac{m}{p_1}) \\
&= p_1 j \text{ for some } j \in \mathbb{Z}
\end{aligned}
$$

   Therefore, $p_1 \mid 1$, which is a contradiction.

$\triangle$

6. Two primes p and q with $p < q$ are called twin primes if $p + 2 = q$. If p and q are twin primes with $3 < p < q$, prove that $6 \mid p + 1$.

   We can take any three consecutive numbers starting with a prime p where $p + 2 = q$ is also prime. We know that any prime number greater than 3 is even, so it is divisible by two. We also know that if we take three consecutive numbers, one of them has to be divisible by 3, since it will either have a remainder of 0, 1, or 2. Since p is prime and $p + 2$ is prime, then $p + 1$ must be divisible by three. Therefore $p + 1$ must be divisible by 6, or $6|p + 1$.