Math 4400 Homework 4

Due: Monday, June 12th, 2017

Feel free to work with your classmates, but everyone must turn in their own assignment. Please make a note of who you worked with on each problem. Let me know if you find a typo, or you're stuck on any of the problems.

1. Let $a, b \in \mathbb{Z}$ be nonzero. Then a and b can both be factored into primes. Let $p_1, \ldots, p_n$ be all of the *distinct* primes appearing in the factorizations of either a or b. It follows from uniqueness of factorization that there exist unique numbers $e_1, \ldots, e_n \in \mathbb{N}$ and $f_1, \ldots, f_n \in \mathbb{N}$ such that $a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ and $b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$ (remember that $\mathbb{N}$ includes 0)

   For example, if $a = 12$ and $b = 28$ then $a = 2 \cdot 2 \cdot 3$ and $b = 2 \cdot 2 \cdot 7$. Then we can set $p_1 = 2, p_2 = 3, p_3 = 7$, and $a = 2^2 \cdot 3^1 \cdot 7^0$, whereas $b = 2^2 \cdot 3^0 \cdot 7^1$.

   (a) (10 points) Prove that $\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_n^{\min(e_n, f_n)}$. (Hint: start by showing that if c is a common factor of a and b, then there exist some integers $h_1, \ldots, h_n \geq 0$ such that $c = p_1^{h_1} \cdots p_n^{h_n}$.)

   (b) (5 points) Can you come up with a similar formula for $\mathrm{lcm}(a, b)$? You don't have to prove it's true in general, but you should show that your formula works for at least two different examples.

2. (10 points) Find all the incongruent solutions to $x^{37} - x \equiv 0 \mod 7$

3. (10 points) Find $\varphi(600)$ and use that to compute $7^{332} \mod 600$, i.e. find an integer x with $0 \leq x < 600$ such that $7^{332} \equiv x \mod 600$.

4. (10 points) Use the Euclidean Algorithm to compute the multiplicative inverse of 131 modulo 1979. Use this to solve the congruence, $131x \equiv 11 \mod 1979$