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 $c = p_1^{h_1} \cdots p_n^{h_n}$.)

Solution: Let c be a common divisor of a and b. There exist unique primes $q_1, \ldots, q_m \in \mathbb{Z}$ and integers $g_1, \ldots, g_m > 0$ such that $c = q_1^{g_1} \cdots q_m^{g_m}$. Then for all i with $1 \leq i \leq m$, $q_i \mid a$. Since q_i is prime, that means that $q_i \mid p_j$ for some j with $1 \leq j \leq m$. But since p_j is prime, that means $q_i = p_j$. This shows that each prime appearing in the factorization of c is in the set $\{p_1, \ldots, p_m\}$. Thus there are some integers $h_1, \ldots, h_m \in \mathbb{N}$ such that $c = p_1^{h_1} \cdots p_m^{h_m}$.

Next we'll show that $h_i \leq \min(e_i, f_i)$ for each i. To see this, suppose $h > \min(e_i, f_i)$. If $\min(e_i, f_i) = e_i$, then, since $c \mid a$, there is some $k \in \mathbb{Z}$ such that $ck = a$. In terms of our prime factorizations, this means

$$p_1^{h_1} \cdots p_m^{h_m} \cdot k = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$

Dividing each side by p^{e_i}, we get

$$p_1^{h_1} \cdots p_i^{h_i - e_i} \cdots p_m^{h_m} \cdot k = p_1^{e_1} p_2^{e_2} \cdot p_{i-1}^{e_{i-1}} p_{i+1}^{e_{i+1}} \cdots p_n^{e_n}$$

But $h_i - e_i \geq 1$, so p_i divides the left-hand side and not the right-hand side. The same argument works if $\min(e_i, f_i) = f_i$: just replace a with b. Thus $h_i \leq \min(e_i, f_i)$.

Further, we see that $p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_n^{\min(e_n,f_n)}$ is a common divisor of a and b. Indeed,

$$p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_n^{\min(e_n,f_n)} \cdot p_1^{e_1 - \min(e_1,f_1)} p_2^{e_2 - \min(e_2,f_2)} \cdots p_n^{e_n - \min(e_n,f_n)} = a,$$

and

$$p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_n^{\min(e_n,f_n)} \cdot p_1^{f_1 - \min(e_1,f_1)} p_2^{f_2 - \min(e_2,f_2)} \cdots p_n^{f_n - \min(e_n,f_n)} = b.$$

Further, $e_i - \min(e_i, f_i) \geq 0$ for all i, so

$$p_1^{e_1 - \min(e_1,f_1)} p_2^{e_2 - \min(e_2,f_2)} \cdots p_n^{e_n - \min(e_n,f_n)}$$

is indeed an integer. Similarly for

$$p_1^{f_1 - \min(e_1,f_1)} p_2^{f_2 - \min(e_2,f_2)} \cdots p_n^{f_n - \min(e_n,f_n)}$$

Since $h_i \leq \min(e_i, f_i)$ for all i, we see that

$$c \leq p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_n^{\min(e_n,f_n)}$$

This completes the proof.

(b) (5 points) Can you come up with a similar formula for $\text{lcm}(a, b)$? 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.

Solution: The correct formula is,

$$\text{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_n^{\max(e_n, f_n)}$$

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

Solution: First, note that $x \equiv 0$ is a solution. Further, if $x \not\equiv 0$, then $x^{37} \equiv x$ by Fermat's little theorem, since $37 = 6 \cdot 6 + 1$. Thus, for all $x \not\equiv 0$, we have $x^{37} - x \equiv x - x \equiv 0$. So every integer is a solution to $x^{37} - x \equiv 0 \mod 7$. In particular, a complete list of incongruent solutions is $0, 1, 2, 3, 4, 5, 6$.

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 $7^{332} \equiv x \mod 600$.

Solution: The prime factorization of 600 is $2^3 \cdot 3 \cdot 5^2$, so

$$\varphi(600) = 600\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 160$$

Note also that $\gcd(600, 7) = 1$ (this is clear from the prime factorization of 600 and problem 1). Thus $7^{332} \equiv 7^{2 \cdot 160 + 2} \equiv 7^2 \equiv 49$.

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

Solution: We perform the Euclidean algorithm on 131 and 1979:

$$\begin{aligned}
1979 &= 15 \cdot 131 + 14 \\
131 &= 9 \cdot 14 + 5 \\
14 &= 2 \cdot 5 + 4 \\
5 &= 1 \cdot 4 + 1 \\
4 &= 4 \cdot 1
\end{aligned}$$

Then we compute:

$$\begin{aligned}
5 - 1 \cdot 4 &= 1 \\
5 - 1 \cdot (14 - 2 \cdot 5) &= 1 \\
3 \cdot 5 - 1 \cdot 14 &= 1 \\
3 \cdot (131 - 9 \cdot 14) - 1 \cdot 14 &= 1 \\
3 \cdot 131 - 28 \cdot 14 &= 1 \\
3 \cdot 131 - 28\,(1979 - 15 \cdot 131) &= 1 \\
423 \cdot 131 - 28 \cdot 1979 &= 1
\end{aligned}$$

Thus, $423 \cdot 131 \equiv 1 \mod 1979$, so 423 is the inverse of 131 modulo 1979.

To solve the equation, we compute:

$$\begin{aligned} & 131x \equiv 11 \mod 1979 \\ \Leftrightarrow & 423 \cdot 131x \equiv 423 \cdot 11 \mod 1979 \\ \Leftrightarrow & 1 \cdot x \equiv 4653 \mod 1979 \end{aligned}$$

So $x \equiv 4653 \mod 1979$. Or, to simplify: $x \equiv 695 \mod 1979$