Math 322 Fall 2019
Number Theory HW 3 Solutions
Due Friday, September 20

You may *not* discuss the starred problem with classmates, though you should of course feel free to discuss it with me as much as you like. Linguistic precision is important for this problem.

($\star$) **Starred Problem:** Let $a_1, \ldots, a_n$ be integers, and let p be a prime. Use induction on n to prove that if $p|a_1 \ldots a_n = \prod_{i=1}^{n} a_i$, then $p|a_i$ for some i.

(We used this result to prove the Fundamental Theorem of Arithmetic, so you cannot use the uniqueness of prime factorizations in your proof).

For the remainder of these problems, I encourage you to collaborate with your classmates, as well as to discuss them with me.

1. Show that if $a = p_1^{e_1} \ldots p_n^{e_n}$ and $b = p_1^{f_1} \ldots p_n^{f_n}$, then $(a, b) = p_1^{\min(e_1,f_1)} \ldots p_n^{\min(e_n,f_n)}$.

   Solution:

   Let $d = p_1^{\min(e_1,f_1)} \ldots p_n^{\min(e_n,f_n)}$. We want to show that d is a common divisor of a and b, and that any other divisor must divide d.

   First we show $d|a$. But note that $e_1 - \min(e_1, f_1)$ is a non-negative integer, so we can write $a = d \cdot p_1^{e_1-\min(e_1,f_1)} \ldots p_n^{e_n-\min(e_n,f_n)}$ and thus $d|a$. Similarly $d|b$.

   Now there are two approaches we can take. The first one is to set $c = (a, b)$. Then since d is a common divisor of a, b, we know that $d|c$. Suppose $d \neq c$; then there is some integer $m > 1$ such that $dm = c$, and m has at least one prime factor p_i, so we can write $dp_i|c$. But then $dp_i|a$ and $dp_i|b$, so $p_i^{\min(e_i,f_i)+1}|p_i^{e_i}$ and $p_i^{\min(e_i,f_i)+1}|p_i^{f_i}$, which is not possible. So $d = c$.

   Alternatively, let $c = p_1^{g_1} \ldots p_n^{g_n}$ be any common divisor of a and b. Then since $c|a$ we see that $g_i \leq e_i$ for each i, and since $c|b$ we see that $g_i \leq f_i$ for each i. Thus $g_i \leq \min(e_i, f_i)$ for each i, and thus $c|d$. Thus since any common divisor of a and b divides d, we know that $d = (a, b)$.

2. State (without proof) a similar result for $\text{lcm}(a, b)$. Use these two results to prove that $(a, b) \cdot \text{lcm}(a, b) = ab$. **Solution:** Statement: let $a = p_1^{e_1} \ldots p_n^{e_n}$ and $b = p_1^{f_1} \ldots p_n^{f_n}$. Then $\text{lcm}(a, b) = p_1^{\max(e_1,f_1)} \ldots p_n^{\max(e_n,f_n)}$.

We know that

$$ab = p_1^{e_1} \dots p_n^{e_n} p_1^{f_1} \dots p_n^{f_n} = p_1^{e_1+f_1} \dots p_n^{e_n+f_n}$$

and

$$(a,b) \cdot \operatorname{lcm}(a,b) = p_1^{\min(e_1,f_1)+\max(e_1,f_1)} \dots p_n^{\min(e_1,f_1)+\max(e_n,f_n)}.$$

So we just need to show that $e_i + f_i = \min(e_i, f_i) + \max(e_i, f_i)$. But if without loss of generality $e_i \leq f_i$, then $\min(e_i, f_i) + \max(e_i, f_i) = e_i + f_i$ as desired.

3. Prove that for any $n \in \mathbb{N}$, there are at least n consecutive composite integers. Hint: consider $(n+1)! + 2$.

   Solution: We notice that $k|(n+1)!$ for $2 \leq k \leq n+1$ (since $(n+1)! = 2 \cdot 3 \cdot \dots \cdot (n+1)$). Thus by the lemma on linear combinations, whenever $2 \leq k \leq n+1$, then $k|(n+1)!+k$. This is a sequence of n consecutive numbers, and each is composite because it is divisible by k for some $k < (n+1)! + k$.

4. Prove that no number of the form n^3+1 where n is an integer is prime except $2 = 1^3+1$.

   Solution: We notice that $n^3 + 1 = (n+1)(n^2 - n + 1)$. For $n > 1$ we have $n + 1 > 1$ and $n^2 - n + 1 > 1$, so $n^3 + 1$ is the product of two factors greater than 1, and thus not prime.

5. Use Fermat's method of squares to factor 14647. (Show your work.)

   Solution: $\sqrt{14647} \approx 121.025$, so we start with 122. We have

$$\begin{aligned} 122^2 - 14647 &= 14844 - 14647 = 237 \\ 123^2 - 14647 &= 15129 - 14647 = 482 \\ 124^2 - 14647 &= 15376 - 14647 = 729 = 27^2 \end{aligned}$$

   So we have

$$14647 = (124 + 27)(124 - 27) = 151 \cdot 97.$$

6. Let S be a set of m integers such that no element of S is congruent to any other element of S mod m. Prove that S is a complete system of residues.

   Solution: Let $S = \{x_1, \dots, x_m\}$. For each i, we know that x_i is congruent to its reduction modulo m, and there are m possible reductions modulo m–the set of integers $\mathbb{Z}/m\mathbb{Z} = \{0, 1, \dots, m-1\}$.

   If two x_i have the same reduction modulo m, then they are congruent to each other, which is a contradiction. So each x_i has a different reduction modulo m. But there are m elements of $\mathbb{Z}/m\mathbb{Z}$, and m elements of S, so each element of $\mathbb{Z}/m\mathbb{Z}$ must be congruent to some element of S.

   Then let a be any integer. a is congruent to its reduction modulo m, which is an element of $\mathbb{Z}/m\mathbb{Z}$, which we just showed is congruent to some element of S. Thus S is a complete system of residues.

7. Let a, b, m, n be integers with $m, n > 0$ and $m|n$. Prove that if $a \equiv b \mod n$, then $a \equiv b \mod m$.

   Solution: Suppose $a \equiv b \mod n$. Then by definition $n|a-b$. But $m|n$ so $m|a-b$, and thus $a \equiv b \mod m$.