Math 322 Fall 2019
Number Theory HW 2 Solutions
Due Friday, September 13

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:** Prove that the greatest common divisor of two even numbers is even.

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

1. Let a and b be integers. For what integers c does the equation $ax + by = c$ have an integer solution? (Hint: pay attention to the form of the left hand side of this equation).

   Solution: The set of linear combinations of a and b is the set of integer multiples of (a, b). Thus this equation has a solution if c is an integer multiple of (a, b), and does not if it is not.

2. Use the Euclidean algorithm, showing all your steps, to compute $(94012, 33396)$. (Feel free to use a calculator).

   Solution:

$$\begin{aligned}(94012, 33396) &= (27220, 33396) = (27220, 6176)\\ &= (2516, 6176) = (2516, 1144)\\ &= (228, 1144) = (228, 4)\\ &= (0, 4) = 4.\end{aligned}$$

3. If n is a positive integer, find (with proof) $(2n^2 + 6n - 4, 2n^2 + 4n - 3)$.

   Solution:

$$\begin{aligned}(2n^2 + 6n - 4, 2n^2 + 4n - 3) &= (2n - 1, 2n^2 + 4n - 3) = (2n - 1, 5n - 3)\\ &= (2n - 1, n - 1) = (n, n - 1) = (1, n - 1)\\ &= (1, 0) = 1.\end{aligned}$$

4. Let p be a prime and n an integer such that p does not divide n. Prove that $\gcd(p, n) = 1$.

   Solution:

   Proof. Let n be a number with $p \not| n$. By the definition of a prime number we know that the only positive divisors of p are 1 and p. We know that p does not divide n, but 1 does divide n, so $\gcd(p, n) = 1$. □

5. Show that if c is an integer, then $\text{lcm}(a, b)|c$ if and only if $a|c$ and $b|c$. (Hint: use the division algorithm).

   Solution: Suppose $\text{lcm}(a, b)|c$. Then since $a|\,\text{lcm}(a, b)$ we know that $a|c$, and since $b|\,\text{lcm}(a, b)$ we know that $b|c$.

   For the converse, there are two approaches: prime factorization, and the division algorithm.

   First approach: Suppose $a|c$ and $b|c$. Suppose $a = p_1^{e_1} \dots p_n^{e_n}$ and $b = p_1^{f_1} \dots p_n^{f_n}$ and $c = p_1^{g_1} \dots p_n^{g_n}$. Then if $a|c$ and $b|c$, for each i we have $e_i, f_i \leq g_i$.

   Now let $\text{lcm}(a, b) = p_1^{h_1} \dots p_n^{h_n}$; clearly $e_i, f_i \leq h_i$ for each i. If $e_i < h_i$ and $f_i < h_i$ for any i, then $a, b|\,\text{lcm}(a, b)/p_i$ which is a contradiction, so $h_i = \max(e_i, f_i) \leq g_i$. Thus $\text{lcm}(a, b)|c$.

   Second approach: suppose $a|c$ and $b|c$, and let $\text{lcm}(a, b) = m$. Then c is a common multiple and m is the least common multiple, so $m \leq c$. Then we can use the Division Algorithm to write $c = mq + r$ for $0 \leq r < m$. But $r = c - mq$, and since $a|c, a|m, b|c, b|m$, by the lemma on linear combinations, $a|r, b|r$, and thus r is a common multiple. But $r < m$ the least common multiple, so $r = 0$. Thus $c = mq$ and thus $m|c$.

6. Let $p > 1$ be an integer with the following property: whenever a, b are integers and $p|ab$, then $p|a$ or $p|b$. Prove that p is prime.

   Solution:

   Suppose p has the given property. Then suppose p has positive factors a and b; that is, suppose $a, b > 0$ with $ab = p$. By the property, either $p|a$ or $p|b$; without loss of generality assume $p|a$. Then $a|p$ and $p|a$ so $p = a$ and $b = 1$.

   Thus the only possible factors of p are p and 1, so p is prime by definition.