Math 322 Fall 2017
Number Theory HW 1 Solutions
Due Friday, September 8

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. Submit this problem on a separate, detached sheet of paper.

$\star$ **Redo Problem:** Show that if a, b, c, d are non-zero integers, and $a|b$ and $c|d$, then $ac|bd$.

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

1. Compute
   - $(6, 8, 10)$ **Solution:** $= 2$
   - $(34, 22)$ **Solution:** $= 2$
   - $(2970, 2925)$ **Solution:** $2970 = 2 \cdot 3^3 \cdot 5 \cdot 11$ and $2925 = 3^2 \cdot 5^2 \cdot 13$ so $(2970, 2925) = 3^2 \cdot 5 = 45$.

2. Prove that if a and b are integers, then $\gcd(a, b)$ exists and is unique.

   Solution: Existence: First, a, b have at least one common divisor because 1 divides every number. Every common divisor of a and b divides b and thus is $\leq b$ (and $\geq -b$). Thus the set of common divisors is finite and therefore has a largest element.

   Uniqueness: The relation $\leq$ is a total order on the set of integers, and thus there is only one largest common divisor.

3. Let a, b, c be integers with $(a, b) = 1$ and $c|(a + b)$. Prove that $(a, c) = (b, c) = 1$.

   Solution: Let $(a, c) = d$. Then $d|c$ and thus $d|(a + b)$, and since $d|a$, by the lemma on linear combinations $d|((a + b) - a) = b$. Thus $d|a, d|b$, so $d|(a, b) = 1$. Thus $(a, c) = d = 1$. An identical argument shows that $(b, c) = 1$.

   Definition 0.1. We say that a set of numbers $a_1, \ldots, a_n$ are *mutually relatively prime* if $\gcd(a_1, \ldots, a_n) = 1$. We say that the set is *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $i \neq j$.

4.
   - Find a triple of numbers (a, b, c) that are mutually relatively prime but not pairwise relatively prime.

     Solution: $(4, 6, 9)$ is one example.
   - Find a quadruple of numbers (a, b, c, d) that are mutually relatively prime, but any subset of three of them is not mutually relatively prime.

     Solution: $30, 42, 70, 105$.

Definition 0.2. If a and b are integers, then we define the *least common multiple* of a and b, written $[a, b]$ or $\text{lcm}(a, b)$, as the least (positive) integer c such that $a|c$ and $b|c$.

5. Let k be a natural number. Prove that $\text{lcm}(ka, kb) = k \cdot \text{lcm}(a, b)$.

   Solution: Suppose c is a common multiple of ka and kb, and thus $ka|c, kb|c$. Then we have integers m, n such that $kam = c, kbn = c$, and then $am = c/k, bn = c/k$ are integers. Thus $a|c/k, b|c/k$ and c/k is a common multiple of a and b.

   Conversely, suppose c/k is a common multiple of a and b (and note we can write any common multiple in this form). Then $a|c/k, b|c/k$, so there are integers m, n such that $am = c/k, bn = c/k$ and thus $amk = bnk = c$ and thus c is a common multiple of ak and bk.

   Thus the set of common multiples of ka and kb is the set of common multiples of a and b multiplied by k; taking the least element of each set, we have $\text{lcm}(ka, kb) = k\,\text{lcm}(a, b)$.