

Math 322 Fall 2017
Number Theory HW 3
Due Friday, September 22

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.

(★) **Starred Problem:** Let a_1, \dots, a_n be integers, and let p be a prime. Prove that if $p|a_1 \dots a_n = \prod_{i=1}^n a_i$, then $p|a_i$ for some i .

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 $a = p_1^{e_1} \dots p_n^{e_n}$ and $b = p_1^{f_1} \dots p_n^{f_n}$, then $(a, b) = p_1^{\min(e_1, f_1)} \dots p_n^{\min(e_n, f_n)}$.
2. State (without proof) a similar result for $\text{lcm}(a, b)$. Use these two results to prove that $(a, b) \cdot \text{lcm}(a, b) = ab$.
3. Prove that for any $n \in \mathbb{N}$, there are at least n consecutive composite integers. Hint: consider $(n+1)! + 2$.
4. Prove that no number of the form $n^3 + 1$ is prime except $2 = 1^3 + 1$.
5. Use Fermat's method of squares to factor 14647.
6. Let S be a set of m integers such that no element of S is congruent to any other element of $S \pmod m$. Prove that 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 $a \equiv b \pmod n$, then $a \equiv b \pmod m$.