Fall 2022, Math 522: Week 3 Problem Set
Due: Friday, September 23rd, 2022
The Fundamental Theorem of Arithmetic

Discussion problems. The problems below should be worked on in class.

(D1) *Proving "uniqueness" in the Fundamental Theorem of Arithmetic.*

(a) Below is a "proof" that there are infinitely many primes. Locate and correct the error.

Proof. By way of contradiction, suppose there are only k primes $p_1, \ldots, p_k$. Let

$$a = p_1 \cdots p_k + 2.$$

For each i, we have $p_i \mid p_1 \cdots p_k$, so $p_i \nmid a$. This means no prime number divide a, and thus a cannot be written as a product of primes. This contradicts the FTA. $\square$

(b) The following is a proof that if p is prime and $p \mid a_1 \cdots a_k$, then $p \mid a_i$ for some i. Write a new proof using induction on k (thus avoiding the shaky "Repeating this process").

Proof. By way of contradiction, suppose p is prime and $p \mid a_1 \cdots a_k$, but $p \nmid a_i$ for every i. Since $p \mid (a_1 \cdots a_{k-1})(a_k)$ and p is prime, either $p \mid a_1 \cdots a_{k-1}$ or $p \mid a_k$. By assumption, $p \nmid a_k$, so $p \mid a_1 \cdots a_{k-1}$. Repeating this process, we conclude $p \mid a_1 a_2$. However, we assumed $p \nmid a_1$ and $p \nmid a_2$, which contradicts the fact that p is prime. $\square$

(c) Fill in the blanks the following proof that if $a \in \mathbb{Z}_{\geq 1}$ satisfies

$$a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r$$

for primes $p_1, \ldots, p_k, q_1, \ldots q_r$, then $k = r$ and, after possibly reordering the right hand side, we have $p_i = q_i$ for each i (this is the "uniqueness" part of the FTA).

Proof. We proceed by induction on a. If $a = 1$, then necessarily $k = r =$ __.

For the inductive step, suppose $a \geq 2$ and that the above claim holds for every $a' < a$. Since $p_k \mid$ ____, by part (b) $p_k \mid q_i$ for some i. Up to reordering, we may assume ____. Since p_k and q_r are both prime, $p_k = q_r$, and applying the inductive hypothesis to

$$a' = p_1 p_2 \cdots p_{k-1} = \underline{\hspace{4cm}}$$

completes the proof. $\square$

(d) Prove or provide a counterexample: if p is prime, $n \geq 1$, and $p^n \mid a^n$, then $p \mid a$.

(e) If the hypothesis "p is prime" is dropped from the previous statement, does that change its truth value? Again, provide a proof or a counterexample.

(D2) *Prime Factorization and GCDs.* The goal of this problem is to prove the following theorem.

Theorem. *If $a = p_1^{r_1} \cdots p_k^{r_k}$ and $b = p_1^{t_1} \cdots p_k^{t_k}$ for some distinct primes $p_1, \ldots, p_k$ with each $r_i, s_i \geq 0$, then $\gcd(a,b) = p_1^{\min(r_1,t_1)} \cdots p_k^{\min(r_k,t_k)}$.*

(a) Given $a, b \in \mathbb{Z}$, is it possible that $\gcd(7a, 7b) = 91$? Is it possible $\gcd(17a, 17b) = 19$? What theorem from the beginning of Monday's class are you using here?

(b) Let $a = 2^2\, 3^1\, 5^1$ and $b = 2^1\, 3^2\, 7^1$. Find (a, b), and verify that your answer is correct by finding *all* divisors of a and b. Also verify this matches the above theorem.

(c) Prove that $\gcd(a, b) = 1$ if and only if there is no prime p such that $p \mid a$ and $p \mid b$. Hint: remember that sometimes it is easier to prove the contrapositive of an implication!

(d) Prove that $p_1^{\min(r_1,t_1)} \cdots p_k^{\min(r_k,t_k)}$ is a divisor of both a and b.

(e) Use the above results to prove $\gcd(a,b) = p_1^{\min(r_1,t_1)} \cdots p_k^{\min(r_k,t_k)}$.

Homework problems. You must submit *all* homework problems in order to receive full credit.

Unless otherwise stated, $a, b, c, d, n \in \mathbb{Z}$ are arbitrary.

(H1) Prove $a \mid b$ if and only if $a^2 \mid b^2$.

(H2) Let $d = \gcd(a, b)$. Use the fundamental theorem of arithmetic to prove that if $a \mid c$ and $b \mid c$, then $ab \mid cd$.

(H3) Prove that if $p > 3$ is prime, then p^2+2 is composite. Hint: consider the possible remainders when dividing p by 3.

(H4) Determine whether each of the following statements is true or false. Prove each true statement, and give a counterexample for each false statement.

(a) If p is prime, $p \mid a^2$, and $p \mid a + b^2$, then $p \mid b$.

(b) If $d = \gcd(a, b)$, then $d^2 = \gcd(a^2, b^2)$.

(c) If $p > 2$ is prime, then $3p + 2$ is prime.