Spring 2021, Math 522: Problem Set 2
Due: Thursday, February 11th, 2021
The Fundamental Theorem of Arithmetic

(D1) *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) Write your answer to Problem (P1) and the above theorem on the board.

(b) 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 Tuesday's class are you using here?

(c) 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.

The goal of the remaining parts of this problem is to prove the above theorem.

(d) 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!

(e) 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.

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

(D2) *Using the Fundamental Theorem of Arithmetic.* The goal of this problem is to practice writing proofs utilizing prime factorization.

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

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 $p_i \nmid a$. Since this holds for every prime, no primes divide a, meaning a cannot be written as a product of primes. This contradicts the fundamental theorem of arithmetic. $\square$

(b) The following is a proof by contradiction that if p is prime and $p \mid a_1 \cdots a_k$, then $p \mid a_i$ for some i. Write an alternative proof that uses induction on k.

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

(d) 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.

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

(H1) Use the Euclidean algorithm to find $\gcd(559, 234)$.

(H2) Prove $a \mid b$ if and only if $a^2 \mid b^2$.

(H3) Let $d = \gcd(a, b)$. Use the fundamental theorem of arithmetic to prove that if $a \mid c$ and $b \mid c$, then $ab \mid cd$.

(H4) Prove that if $p > 3$ is prime, then p^2+2 is composite. Hint: consider the possible remainders when dividing p by 3.

(H5) 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.

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) Suppose $r \in \mathbb{Q}$ and $n \in \mathbb{Z}_{\geq 0}$. Prove that if $r^n \in \mathbb{Z}$, then $r \in \mathbb{Z}$.