Fall 2023, Math 320: Week 2 Problem Set
Due: Thursday, September 14th, 2023
Primes and Unique Factorization

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 numbers 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 <u>on</u>** $\underline{k}$ (to avoid 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 proof of the following claim: 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 assume that the "uniqueness" part of FTA holds every $a' < a$ (this is the inductive hypothesis). Since $p_k \mid$ __________, part (b) implies $p_k \mid$ ____ for some i. Up to reordering of the q's, we may assume $i =$ ____. Since p_k and ____ are prime, $p_k =$ ____, and applying the inductive hypothesis to
$$a' = p_1 p_2 \cdots p_{k-1} = \underline{\hspace{6em}}$$
completes the proof. $\square$

(D2) *Applying the Fundamental Theorem of Arithmetic.*

(a) Fill in the blanks in the following proof that if p is prime, $n \geq 1$, and $p \mid a^n$, then $p \mid a$.

Proof. Let $a = p_1^{r_1} \cdots p_k^{r_k}$ with each p_i prime and $r_i > 0$. Then $a^n = p_1^{\_\_} \cdots p_k^{\_\_}$. Since $p \mid a$, we have $a = cp$ for some $c \in \mathbb{Z}$. By uniqueness in FTA, $p = p_i$ for some i, meaning $a = p(p_1^{\_\_} \cdots p_i^{\_\_\_\_} \cdots p_k^{\_\_})$, which implies $p \mid a$. $\square$

(b) If the hypothesis "p is prime" is dropped from the previous statement, is the statement still true? Provide a proof or a counterexample.

(c) Let $a = 2^3\, 3^2\, 5^2$ and $b = 2^1\, 3^4\, 7^1$. Find $\gcd(a, b)$, and verify that your answer is correct by finding *all* common divisors of a and b.

(d) Fill in the blank: 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 $r_i, t_i \geq 0$, then $\gcd(a, b) = p_1^{u_1} \cdots p_k^{u_k}$, where $u_i =$ ___________ for each i. Hint: how can we tell if $a \mid b$ in terms of the r_i's and t_i's?

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

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 and $p \in \mathbb{Z}_{\geq 2}$ is prime.

(H1) Prove that if $p > 3$ is prime, then p^2+2 is composite. Hint: consider the possible remainders when dividing p by 3.

(H2) Prove that any **nonzero** $n \in \mathbb{Z}$ can be written uniquely in the form $n = 2^k m$ for some $k \in \mathbb{Z}_{\geq 0}$ and odd $m \in \mathbb{Z}$.

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

(b) 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) Prove that if $p \geq 5$ and $q \geq 5$ are prime, then $24 \mid (p^2 - q^2)$.