Fall 2018, Math 320: Week 2 Problem Set
Due: Tuesday, September 11th, 2018
The Fundamental Theorem of Arithmetic

Discussion problems. The problems below should be completed in class.

(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 $(a, b) = p_1^{\min(r_1,t_1)} \cdots p_k^{\min(r_k,t_k)}$.*

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

(b) 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) Fill in the gaps in the following proof that if $(a, b) = d$, then $(a/d, b/d) = 1$.

Proof. Since $d \mid a$ and $d \mid b$, $\frac{a}{d}$ and $\frac{b}{d}$ are integers. By Problem (R3) from last week,

$$d = (a, b) = (d\tfrac{a}{d}, d\tfrac{b}{d}) = \underline{\hspace{3cm}}$$

and dividing both sides by d completes the proof. □

(d) Prove that $(a, b) = 1$ 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 a statement!

(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 $(a, b) = p_1^{\min(r_1,t_1)} \cdots p_k^{\min(r_k,t_k)}$.

(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. □

(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. □

(c) Use Problem (D1) to prove that if $d = (a, b)$, then $d^2 = (a^2, b^2)$.

(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 above statement, does that change its truth value? Again, provide a proof or a counterexample.

Required problems. As the name suggests, you must submit *all* required problems with this homework set in order to receive full credit.

(R1) Use the Euclidean algorithm to find $(533, 234)$.

(R2) Prove that any $n \in \mathbb{Z}_{\geq 1}$ can be written in the form $n = 2^k m$ for some $k \geq 0$ and odd m.

(R3) Prove that if $2^p - 1$ is prime, then p is prime. Hint: prove the contrapositive.

(R4) Prove that if $c \mid ab$ and $(a, c) = d$, then $c \mid db$.

(R5) 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, $p \mid a$, and $p \mid a^2 + b^2$, then $p \mid b$.

(b) If p is prime, then $2^p - 1$ is prime.

Selection problems. You are required to submit all parts of *one* selection problem with this problem set. You may submit additional selection problems if you wish, but please indicate what you want graded. Although I am happy to provide written feedback on all submitted work, no extra credit will be awarded for completing additional selection problems.

(S1) Prove that if $n > 2$, then there exists a prime p such that $n < p < n!$.

(S2) Suppose $p, q \geq 5$ are primes. Prove that $24 \mid p^2 - q^2$.

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) Characterize which $a, b \in \mathbb{Z}$ satisfy $(a, b) = (a - b, a + b)$ in terms of prime factorizations. Note: your answer should include a *concise* "if and only if" statement, *and* a proof.