Math 412. Adventure sheet on The Fundamental Theorem of Arithmetic

THE FUNDAMENTAL THEOREM OF ARITHMETIC:
Every integer can be factored into primes in an essentially unique way.

This theorem is so familiar that you may think it obvious. It is not! More precisely:

DEFINITION: A nonzero integer $p \neq \pm 1$ is **prime** if its only divisors are ± 1 and $\pm p$.

THE FUNDAMENTAL THEOREM OF ARITHMETIC: A nonzero integer $n \neq \pm 1$ can be written as a product of primes; moreover, if

$$p_1 \cdots p_s \text{ and } q_1 \cdots q_t$$

are two factorizations of n into primes, then, $s = t$ and there exists a reordering of the $\{q_j\}$ such that $q_i = \pm p_i$ for all i.

A. WARMUP: Find two different factorizations of -24 into primes (note that these are the same up to reordering). How do we factor -17 into an (essentially unique) product of primes?

B. In this problem we **assume** the following

THEOREM 1.5: *A nonzero integer $a \neq \pm 1$ is prime if and only if it has the following property:*

($\star$) *if $a|bc$, then $a|b$ or $a|c$.*

Note that a being prime is a statement about the numbers that divide a, whereas property ($\star$) is a statement about numbers that a divides.

(1) Observe that $6|(9 \times 4)$. Use this observation and Theorem 1.5 to show that 6 is not prime.
(2) For the composite number $a = 81$, find $b, c \in \mathbb{Z}$ so that property ($\star$) fails for a with your b and c.
(3) Prove the following Corollary of Theorem 1.5: *If $p \in \mathbb{Z}$ is prime, and $p|(a_1 \cdots a_n)$ where all $a_i \in \mathbb{Z}$, then $p|a_i$ for some i.*[1]

C. PROOF OF THE FUNDAMENTAL THEOREM, PART I

(1) Explain why it suffices to prove the Fundamental Theorem for **positive** n.
(2) The Fundamental Theorem is basically an "existence" and "uniqueness" statement. As usual, we focus of proving each separately. Discuss with your workmates precisely what is the "existence" part of the theorem? What is the "uniqueness" part of the theorem?
(3) Consider the set $\mathcal{S}$ be the set of all integers greater than 1 that are **not** products of primes. To make progress on the proof of the Fundamental Theorem, what do we want to show about $\mathcal{S}$?
(4) Show that any element of $\mathcal{S}$ is a **composite** integer.[2]
(5) Show that if a and b are integers greater than 1, and $ab \in \mathcal{S}$, then a or b is in $\mathcal{S}$.
(6) Prove Theorem 1.7: *Every integer (except $0, 1$ and -1) is a product of primes.*[3]

[1] Hint: induce on n.
[2] A number is **composite** if is not prime; that is, it factors into two numbers that are both not ± 1 or $\pm$ itself.
[3] Hint: If not, consider the smallest element of $\mathcal{S}$, then find a smaller element of $\mathcal{S}$ for a contradiction.

D. PROOF OF THE FUNDAMENTAL THEOREM, PART II. In C, you proved that every integer is a product of primes. We now need to see that this product is *essentially unique.* Assume Theorem 1.5 from Part B for now.

(1) Suppose that $p_1 \cdots p_s$ and $q_1 \cdots q_t$ are two different factorizations of an integer n into primes. Using (the Corollary) to Theorem 1.5, explain why p_1 must divide one of the q_i. Now use the definition on page 1 to explain p_1 must be $\pm q_i$ for some i.
(2) Finish the uniqueness part of the proof of the Fundamental Theorem.[4]

E. PROOF OF THEOREM 1.5. The only missing piece of the proof of the Fundamental Theorem is now the proof of **Theorem 1.5:** *A nonzero integer $a \neq \pm 1$ is prime if and only if it has the following property:*

($\star$) *if $a|bc$, then $a|b$ or $a|c$.*

(1) If $a|d$ and $d|a$, how are a and d related?
(2) Suppose that a has property $(\star)$, and that $d|a$. Write $a = de$ for some e, and notice that $a|de$. What does the fact that a has property $(\star)$ say here?
(3) Prove that if a has property $(\star)$, then a is prime.
(4) Suppose that p is prime and $b \in \mathbb{Z}$ is arbitrary. What are the possible values of (p, b)?
(5) Prove that if p is prime, then p has property $(\star)$.
(6) Note that you have now proven Theorem 1.5, and hence completed the proof of the Fundamental Theorem!

F. THE GREATEST COMMON DIVISOR RETURNS. Consider positive integers a and b, and write

$$a = p_1^{a_1} \cdots p_n^{a_n} \quad \text{and} \quad b = p_1^{b_1} \cdots p_n^{b_n}$$

where $a_1, \ldots, a_n, b_1, \ldots, b_n \geqslant 0$ and $p_1, \ldots, p_n > 0$ are primes.

(1) Can you list all the common divisors of a and b?
(2) Write (a, b) in terms of $p_1, \ldots, p_n, a_1, \ldots, a_n, b_1, \ldots, b_n$.
(3) Prove that if d is any common divisor of a and b, then $d|(a, b)$.

[4]Hint: Aiming for proof by contradiction, choose the **smallest positive** n that has two essentially different factorization into primes. Get a contradiction by finding a smaller one.