The Fundamental Theorem of Arithmetic

Learning Objectives. By the end of class, students will be able to:

- Prove the Fundamental Theorem of Arithmetic
- Prove $\sqrt{2}$ is irrational .

Read Strayer, Section 1.5 through Proposition 1.17

Turn in

- Answer these questions about the proof of the Fundamental Theorem of Arithmetic (taken from Helping Undergraduates Learn to Read Mathematics):
  - Can you write a brief outline (maybe 1/10 as long as the theorem) giving the logic of the argument – proof by contradiction, induction on n, etc.? (This is KEY.)
  - What mathematical raw materials are used in the proof? (Do we need a lemma? Do we need a new definition? A powerful theorem? and do you recall how to prove it? Is the full generality of that theorem needed, or just a weak version?)
  - What does the proof tell you about why the theorem holds?
  - Where is each of the hypotheses used in the proof?
  - Can you think of other questions to ask yourself?
- Strayer states that the proof of **??** is "obvious from the Fundamental Theorem of Arithmetic and the definitions of (a, b) and $[a, b]$." Is this true? If so, why? If not, fill in the gaps.

Solution: Answers to both questions will vary between students.

Theorem 1 (Fundamental Theorem of Arithmetic)**.** Every integer greater than one can be written in the form $p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ where the p_i are distinct prime numbers and the a_i are positive integers. This factorization into primes is unique up to the ordering of the terms.

Proof We will show that every integer n greater than 1 has a prime factorization. First, note that all primes are already in the desired form. We will use induction to show that every composite integer can be factored into the product of primes. When $n = 4$, we can write $n = 2^2$, so 4 has the desired form.

Assume that for all integers k with $1 < k < n$, k can be written in the form $p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ where the p_i are distinct prime numbers and the a_i are positive integers. If n is prime, we are done, otherwise there exists $a, b \in \mathbb{Z}$ with $1 < a, b < n$ such that $n = ab$. By the induction hypothesis, there exist primes $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ and positive integers $a_1, a_2, \ldots, a_r, b_1, b_2, \ldots b_s$ such that $a = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ and $b = q_1^{b_1}q_2^{a_2}\cdots q_s^{b_a}$. Then

$$n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}q_1^{b_1}q_2^{a_2}\cdots q_s^{b_a}.$$

■

We will use an idea similar to the proof of the Fundamental Theorem of Arithmetic to proof the following:

In-class Problem 1

Learning outcomes:
Author(s): Claire Merriman

Proposition 1. $\sqrt{2}$ is irrational

Put the following steps in order:

10 Therefore, $\sqrt{2}$ is not rational. 2 Assume that $\sqrt{2}$ is rational, ie, there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = \frac{p}{q}$.
6 Therefore there exists $k \in \mathbb{Z}$ such that $p = 2k$ by (definition of $2 \mid p$ ✓/ definition of $2 \mid p^2$/ **??**/ prime factorization)
4 Then (include to remove fractions and the radical) $2q^2 = p^2$.
5 Then $2 \mid p^2$ by definition of divisibility and $2 \mid p$ by (definition of $2 \mid p$/ definition of $2 \mid p^2$/ **??** ✓/ prime factorization
)
9 This contradicts our assumption that ($\sqrt{2} = \frac{p}{q}$. / $2q^2 = p^2$/ $(p, q) = 1$ ✓) 7 Then (more algebraic manipulations)
$2q^2 = 4k^2$ and $q^2 = 2k^2$.
1 We proceed by contradiction.
8 Then $2 \mid q^2$ and $2 \mid q$ by (definition of $2 \mid q$/ definition of $2 \mid q^2$/ **??** ✓/ prime factorization) and (definition of $2 \mid q$
✓/ definition of $2 \mid q^2$/ **??**/ prime factorization)
3 Without loss of generality, we may assume $(p, q) = 1$, since

Finally, work two groups. Each group will be assigned one of the following question.

In-class Problem 2 Let p be prime.

(a) If $(a, b) = p$, what are the possible values of (a^2, b)? Of (a^3, b)? Of (a^2, b^3)?

(b) If $(a, b) = p$ and $(b, p^3) = p^2$, find (ab, p^4) and $(a + b, p^4)$.