Math 412. 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 and sign). How do we factor -17 into an (essentially unique) product of primes?

A few possibilities to factor -24:

$$-24 = -2*2*2*3 = 2*2*2*-3 = -3*2*2*2 = -2*-3*-2*2.$$

The prime factorization of -17 is simply -17.

B. In this problem we **assume** THEOREM 1.5: *A nonzero integer $a \neq \pm 1$ is prime if and only if it has the following property:*

$$(\star) \qquad \text{if } a|bc, \text{ then } a|b \text{ or } a|c.$$

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.

6 does not divide 9 and 6 does not divide 4. Thus with $a = 6$, $b = 9$, and $c = 4$, the "if" part of $\star$ holds, while the "then" conclusion fails. Thus the implication in $\star$ fails for $a = 6$, so 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.

Take $b = c = 9$. Then $81|(9 * 9)$ but $81 \nmid 9$.

(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]

We will use induction on n. If $n = 1$, this just says that $p|a_1$ implies $p|a_1$, a tautology. Suppose we know the statement is true for n, and suppose $p|(a_1 \cdots a_n a_{n+1})$. Then, by $(\star)$, $p|(a_1 \cdots a_n)$ or $p|a_{n+1}$. In the first case, by hypothesis, $p|a_i$ for some $1 \leqslant i \leqslant n$, and the conclusion holds in the latter case as well.

C. Proof of the Fundamental Theorem, Part I

(1) Explain why it suffices to prove the Fundamental Theorem for **positive** n.

Suppose we know prime factorizations for all positive $m > 1$, and we want to show that any negative $n < -1$ has a prime factorization. Then, for such an n, $-n > 1$, so we can write $-n = p_1 \cdots p_t$ by assumption. Then $n = (-p_1)p_2 \cdots p_t$ is a prime factorization of 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 $\mathcal{S}$?

[1] Hint: use induction on n.

That $\mathcal{S}$ is empty!

(4) Show that every element of $\mathcal{S}$ is a **composite** integer.[2]

Note that if p is prime, it cannot be an element of $\mathcal{S}$: any prime p has the trivial factorization p. Thus, if $\mathcal{S}$ is nonempty, any of its elements is composite.

(5) Show that if a and b are integers greater than 1, and $ab \in \mathcal{S}$, then a or b is in $\mathcal{S}$.

We prove the *contrapositive:* if a and b are not in $\mathcal{S}$, then $ab \notin \mathcal{S}$. If a and b are not in $\mathcal{S}$, then they admit prime factorizations,

$$a = p_1 \cdots p_s \quad \text{and} \quad b = q_1 \cdots q_t.$$

Then, $ab = p_1 \cdots p_s q_1 \ldots q_t$ is a prime factorization.

(6) Prove Theorem 1.7: *Every integer (except* $0, 1$ *and* -1*) is a product of primes.*[3]

We proceed by contradiction. If not, $\mathcal{S}$ is nonempty, so it has a minimal element s. As noted in (4), s is composite: we can write $s = ab$ with $a, b > 1$. By (5), either a or b is in $\mathcal{S}$. But, $a < s$ and $b < s$, which contradicts that s is minimal in $\mathcal{S}$. Thus, by contracdiction, we see that $\mathcal{S}$ is empty. This implies the theorem.

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] A number is **composite** if is not prime; that is, it factors into two numbers that are both not ±1 or ± itself.

[3] Hint: If not, consider the smallest element of $\mathcal{S}$, then find a smaller element of $\mathcal{S}$ for a contradiction.

We know that $p_1|(q_1 \cdots q_t)$, so, by the Corollary, $p_1|q_i$ for some i. Since q_i is prime, $p_1 = \pm q_i$ or $p_1 = \pm 1$. Since $p_1 \neq \pm 1$, we must have $p_1 = \pm q_i$.

(2) Finish the uniqueness part of the proof of the Fundamental Theorem.[4]

We argue by contradiction: suppose that n is the smallest positive number that has two prime factorizations that are not essentially the same:

$$n = p_1 \cdots p_s = q_1 \cdots q_t.$$

By the previous part, $p_1 = \pm q_i$. Consider

$$n/p_1 = p_2 \cdots p_s = q_1 \cdots \widehat{q_i} \cdots q_t.$$

After reordering and renumbering the q's, we can take $i = 1$ above, so

$$n/p_1 = p_2 \cdots p_s = q_2 \cdots q_t.$$

Since $n/p_1 < n$, we know that there is a reordering of $\{q_2, \ldots, q_n\}$ such that $q_i = \pm p_i$ for all $i > 1$. Put together, this gives a reordering of $\{q_1, \ldots, q_n\}$ such that $q_i = \pm p_i$ for all $i \geq 1$. This contradicts that the two given factorizations are not essentially the same.

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?

$d = \pm a$

(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?

[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.

$a|d$ or $a|e$.

(3) Prove that if a has property $(\star)$, then a is prime.

If $d|a$, write $a = de$. As in (2), this in particular means $a|de$ so that by property $(\star)$, we have $a|d$ or $a|e$. On the other hand, since $a = de$, we have $d|a$ and $e|a$. It follows then that either $d = \pm a$ or $e = \pm a$. In the latter case, $d = \pm 1$. We've thus shown that if $d|a$, then $d = \pm a$ or ± 1, which exactly says that a is prime.

(4) Suppose that p is prime and $b \in \mathbb{Z}$ is arbitrary. What are the possible values of (p, b)?

If $p|b$, then the gcd is p, otherwise, it is 1.

(5) Prove that if p is prime, then p has property $(\star)$.

Suppose that p is prime, and $p|bc$. We need to show that $p|b$ or $p|c$. If $p \nmid b$, then $(p, b) = 1$. By Theorem 1.4, $p|c$.

(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

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

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?

The common divisors of a and b are all the integers of the form

$$\pm p_1^{c_1} \cdots p_n^{c_n}$$

where for each $1 \leqslant i \leqslant n$ we have $0 \leqslant c_i \leqslant \min\{a_i, b_i\}$.

(2) Write (a, b) in terms of $p_1, \ldots, p_n, a_1, \ldots, a_n, b_1, \ldots, b_n$.

$$(a,b) = p_1^{\min\{a_1,b_1\}} \cdots p_n^{\min\{a_n,b_n\}}.$$

(3) Prove that if d is any common divisor of a and b, then $d|(a,b)$.

By (1), we can write $d = \pm p_1^{c_1} \cdots p_n^{c_n}$, where $0 \leqslant c_i \leqslant \min\{a_i, b_i\}$ for each i. Then $p_i^{c_i} | p_i^{\min\{a_i,b_i\}}$, and

$$d = \pm p_1^{c_1} \cdots p_n^{c_n} | p_1^{\min\{a_1,b_1\}} \cdots p_n^{\min\{a_n,b_n\}} = (a,b).$$