Prime numbers

Fundamental theorem of arithmetic

We have already seen techniques for factoring numbers into products of primes.

The Fundamental Theorem of Arithmetic states that this factorization is unique - you can’t come up with two different ways to write the prime factorization of a number, and if two numbers have the same factorization, then they must be the same number.

Fundamental theorem of arithmetic

Theorem:

Let $n$ be any integer greater than 1. There are distinct primes $p_1, p_2, \ldots, p_m$ and positive exponents $k_1, k_2, \ldots, k_m$ such that

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}.$$ 

Furthermore, such a factorization is unique except for the order of the factors.

To prove the theorem, we need to establish a couple of propositions. Proofs of all of these are lengthy enough that outlines appear in the notes, but not on the slides. See also Nicodemi, pp. 28-29.

Proposition:

Let $p$ be a positive integer. Then $p$ is prime if and only if for all integers $a$ and $b$, if $p$ divides $ab$, then $p$ either divides $a$ or $p$ divides $b$.

Note: this is the inclusive “or” - it is possible that $p$ divides both.

Example:

Take the prime $p = 5$ and the number 50. There’s a couple different ways to factor 50: $50 = 5 \cdot 10$, or $50 = 2 \cdot 25$. What the above theorem guarantees is that since 5|50, it must divide at least one of the factors of 50 for any possible factorization of 50.

Proof logic:

- It’s an “if and only if” statement, so it must be proven in both directions.

- The proof of “Suppose that $p$ is prime. Then for all integers $a$ and $b$, if $p$ divides $ab$, then $p$ either divides $a$ or $p$ divides $b$” proceeds directly:
  - Suppose $p$ is prime. Suppose that $p|ab$.
  - If $p|a$, then we’re done.
  - If $p \not| a$, then gcd($p, a$) = 1 and Euclid’s Lemma states that $p|b$. 
• The converse (other direction of the iff) would be “Suppose that \( p \) is some number with the property that if \( p \) divides \( ab \), then \( p \) either divides \( a \) or \( p \) divides \( b \). Then \( p \) is prime.”

• The proof of the converse proceeds indirectly:
  – Suppose \( p \) is not prime.
  – Then \( p \) can be factored as \( p = ab \), and \( p \) does not divide either \( a \) or \( b \).

**Proposition:**

Suppose that \( p \) is prime and that \( p \) divides \( a_1a_2...a_n \). Then \( p \) divides \( a_k \) for some \( k \) such that \( 1 \leq k \leq n \). Also, if \( a_k \) is prime, then \( p = a_k \).

**Note:** This proposition is simply an extension of the previous one. If \( p \) divides some number, and that number can be factored in a certain way, then \( p \) either divides one of the factors, or \( p \) is one of the factors.

**Note:** The Nicodemi text states that this “follows by induction” without showing the induction proof. For completeness sake, let’s have it here. This is an example of the use of the Principle of Strong Induction.

Basis Step: \((k = 2)\) Suppose \( p \mid a_1a_2 \). Then by the preceding proposition, \( p \mid a_1 \) or \( p \mid a_2 \). Whichever one \( p \) divides, if it happens to be prime itself, then it has no divisors other than itself and 1, so \( p \) must equal it.

Inductive Step:

• Suppose that \( p \mid a_1a_2...a_n \) implies that \( p \mid a_k \) for some \( k \) such that \( 1 \leq k \leq n \).

• We wish to show that if \( p \mid a_1a_2...a_n a_{n+1} \), then \( p \mid a_k \) for some \( k \) such that \( 1 \leq k \leq n+1 \).

• Suppose that \( p \mid a_1a_2...a_n a_{n+1} \). Then \( p \mid ba_{n+1} \), where \( b = a_1a_2...a_n \). By the preceding proposition, either \( p \mid b \) or \( p \mid a_{n+1} \).
  – If \( p \mid b \), then \( p \mid a_1a_2...a_n \), and by the induction hypothesis, \( p \mid a_k \) for some \( k \) such that \( 1 \leq k \leq n \).
  – On the other hand, if \( p \mid a_{n+1} \), then \( p \mid a_k \) for some \( k = n + 1 \).
  – Taken together, \( p \mid a_k \) for some \( k \) such that \( 1 \leq k \leq n + 1 \)

• And, as before, if \( a_k \) is prime, it has no divisors other than 1 and \( a_k \), so if \( p \mid a_k \), then \( p = a_k \).
Proving the fundamental theorem

With the preceding propositions, we can prove the fundamental theorem. This is also an induction proof. A key thing to notice is that this is an example of an “existence and uniqueness” proof.

I’m going to use a version of the proof that I think is a little easier to follow. The gathering of repeated factors into exponents isn’t really a necessary part of the theorem, just a fact of arithmetic notation - there’s no difference in asserting that

\[ 250 = 2 \cdot 5 \cdot 5 \cdot 5 \]

vs.

\[ 250 = 2 \cdot 5^3 \]

other than that the second one is more compact to write.

Existence: The simplest statement of the existence part of the Fundamental Theorem of Arithmetic is

Every natural number \( n \) greater than one can be written as the product of primes.

Basis step: \( P(2) \) holds: Since 2 itself is prime, \( 2 = 2 \) can be written as the product of one prime, itself. (Yes, we allow “product” to possibly collapse down to a single number. It counts.)

Induction step:

- Assume that \( P(j) \) holds for all \( j \leq n \) (this is a strong induction): Assume a natural number \( j \) can be written as a product of primes for all \( j \leq n \).
- We wish to show \( P(n + 1) \) holds: We wish to show that \( n + 1 \) can be written as a product of primes.
- Consider \( n + 1 \). There are two cases:
  - \( n + 1 \) is prime. Then it can be written as itself, and we are done.
  - \( n + 1 \) is composite. Then it can be factored into \( n + 1 = ab \), and both \( a \) and \( b \) are greater than 1, and less than \( n + 1 \). Since \( a < n + 1 \), \( a \leq n \), and the induction hypothesis says \( a \) can be written as a product of primes. Similarly, \( b \) can be written as a product of primes. So \( n + 1 \) is the product of products of primes; \( n + 1 \) can be written as a product of primes.

By induction, every natural number \( n \) greater than one can be written as the product of primes.

Uniqueness: The uniqueness part can be done by contradiction:

Suppose we have a number \( n \) that has two distinct prime factorizations, both

\[ n = p_1p_2p_3...p_s \]

and

\[ n = q_1q_2q_3...q_t \]
The next bit is easier to explain than it is to notate. Since the factorizations are assumed to be distinct, there have to be some primes in the $p$ factorization that don’t match the primes in the $q$ factorization. As an example, suppose that all the $p$ factors and $q$ factors were equal, except that maybe $p_2 \neq q_2$, and $p_7 \neq q_7$. If you set up the equation

$$p_1 p_2 p_3 \ldots p_s = n = q_1 q_2 q_3 \ldots q_t$$

you’d be able to cancel all the like factors on either side, leaving you with just

$$p_2 p_7 = q_2 q_7$$

That would be a problem, since it would imply (for example) that $p_7$ divided either $q_2$ or $q_7$, and it can’t, since primes can’t be divided by primes other than themselves.

To notate this correctly, you go to subscripting the subscripts; if you set up the equality

$$p_1 p_2 p_3 \ldots p_s = n = q_1 q_2 q_3 \ldots q_t$$

and cancel all common primes from both sides of the equation, you are left with

$$p_{i1} p_{i2} \ldots p_{iu} = q_{j1} q_{j2} \ldots q_{jv}$$

(there are some number of $p_i$’s on the $p$ side that don’t cancel against some number of $q_j$’s on the $q$ side).

So $p_{i1}$ must divide some $q_{jv}$, which is a contradiction, since all the factors remaining are distinct primes.

**Consequences of the fundamental theorem**

One thing of note about the theorem is it doesn’t tell you how to find a prime factorization, merely that you can. Fortunately, you already know how (keep factoring until you have a product of primes).

**Corollary:**

Every positive rational number can be expressed uniquely as $\frac{m}{n}$, where $m$ and $n$ are relatively prime natural numbers.

**Theorem:**

There is no rational number whose square is 2 [i.e. $\sqrt{2}$ is irrational].