Fundamental theorem of arithmetic

In number theory, the fundamental theorem of arithmetic (or the unique-prime-factorization theorem) states that any integer greater than 1 can be written as a unique product (up to ordering of the factors) of prime numbers. For example,

\[6936 = 2^3 \times 3^1 \times 17^2,\]
\[1200 = 2^4 \times 3^1 \times 5^2.\]

Proof of existence of a prime factorization is straightforward; proof of uniqueness is more challenging. Some proofs use the fact that if a prime number \(p\) divides the product of two natural numbers \(a\) and \(b\), then \(p\) divides either \(a\) or \(b\), a statement known as Euclid's lemma. Since multiplication on the integers is both commutative and associative, it does not matter in what way we write a number greater than 1 as the product of primes; it is common to write the (prime) factors in the order of smallest to largest.

Some natural extensions of the hypothesis of this theorem allow any non-zero integer to be expressed as the product of "prime numbers" and "invertibles". For example, 1 and −1 are allowed to be factors of such representations (although they are not considered to be prime). In this way, one can extend the Fundamental Theorem of Arithmetic to any Euclidean domain or principal ideal domain bearing in mind certain alterations to the hypothesis of the theorem. A ring in which the Fundamental Theorem of Arithmetic holds is called a unique factorization domain.

Many authors assume 1 to be a natural number that has no prime factorization. Thus Theorem 1 of Hardy & Wright (1979) takes the form, "Every positive integer, except 1, is a product of one or more primes," and Theorem 2 (their "Fundamental") asserts uniqueness. By convention, the number 1 is not itself prime, but since it is the product of no numbers, it is often convenient to include it in the theorem by the empty product rule. (See, for example, Calculating the gcd.)

Applications

The fundamental theorem of arithmetic establishes the importance of prime numbers. Prime numbers are the basic building blocks of any positive integer, in the sense that each positive integer can be constructed from the product of primes with one unique construction. Finding the prime factorization of an integer allows derivation of all its divisors, both prime and non-prime. This property of uniqueness is powerful, as the factorization can be thought of as a key for a number. This is why it can be used to build powerful encryption techniques such as RSA.

For example, the above factorization of 6936 shows that any positive divisor of 6936 must have the form \(2^a \times 3^b \times 17^c\), where \(a\) takes one of the 4 values in \(\{0, 1, 2, 3\}\), where \(b\) takes one of the 2 values in \(\{0, 1\}\), and where \(c\) takes one of the 3 values in \(\{0, 1, 2\}\). Multiplying the numbers of independent options together produces a total of \(4 \times 2 \times 3 = 24\) positive divisors.

Once the prime factorizations of two numbers are known, their greatest common divisor and least common multiple can be found quickly. For instance, from the above it is shown that the greatest common divisor of 6936 and 1200 is \(2^3 \times 3 = 24\). However, if the prime factorizations are not known, the use of the Euclidean algorithm generally requires much less calculation than factoring the two numbers.

The fundamental theorem ensures that additive and multiplicative arithmetic functions are completely determined by their values on the powers of prime numbers.

It may be important to note that Egyptians like Ahmes used earlier practical aspects of the factoring, such as the least common multiple, allowing a long tradition to develop, as formalized by Euclid, and rigorously proven by Carl Friedrich Gauss.

Although at first sight the theorem seems 'obvious', it does not hold in more general number systems, including many rings of algebraic integers. This was first pointed out by Ernst Kummer in 1843, in his work on Fermat's Last
Theorem. The recognition of this failure is one of the earliest developments in algebraic number theory.

Euclid's proof

The proof consists of two steps. In the first step every number is shown to be a product of zero or more primes. In the second step, the proof shows that any two representations may be unified into a single representation.

Non-prime composite numbers

Proof by contradiction via minimal counterexample: Suppose there were positive integers which cannot be written as a product of primes. Then by the well-ordering principle there must be a smallest such number, \( n \). Because of the empty-product convention above, \( n \) cannot be 1. Also, \( n \) cannot be a prime number, since any prime number is a product of a single prime: itself. So \( n \) must be a composite number. Thus

\[ n = a \cdot b, \]

where both \( a \) and \( b \) are positive integers smaller than \( n \). Since \( n \) is the smallest number which cannot be written as a product of primes, both \( a \) and \( b \) can be written as products of primes. But then

\[ n = a \cdot b, \]

can be written as a product of primes as well, simply by combining the factorizations of \( a \) and \( b \); but this contradicts our supposition. Hence, all positive integers can be written as a product of primes.

Proof of uniqueness

The key step in proving uniqueness is Euclid's proposition 30 of book 7 (known as Euclid's lemma), which states that, for any prime number \( p \) and any natural numbers \( a, b \): if \( p \) divides \( ab \) then \( p \) divides \( a \) or \( p \) divides \( b \).

This may be proved as follows:

- Suppose that a prime \( p \) divides \( ab \) (where \( a, b \) are natural numbers) but does not divide \( a \). We must prove that \( p \) divides \( b \).
- Since \( p \) does not divide \( a \), and \( p \) is prime, the greatest common divisor of \( p \) and \( a \) is 1.
- By Bézout's identity, it follows that for some integers \( x, y \) (possibly negative), \( px + ay = 1 \).
- Multiplying both sides by \( b \), \( pxb + aby = b \).
- Since \( p \) divides \( ab \), \( p \) divides \( (ab)y \)
- Since \( p \) divides both summands on the left, \( p \) divides \( b \).

A proof of the uniqueness of the prime factorization of a given integer proceeds as follows. Let \( s \) be the smallest natural number that can be written as (at least) two different products of prime numbers. Denote these two factorizations of \( s \) as \( p_1 \cdots p_m \) and \( q_1 \cdots q_n \), such that \( s = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n \). Both \( q_1 \) and \( q_2 \cdots q_n \) must have unique prime factorizations (since both are smaller than \( s \)). By Euclid's proposition either \( p_1 \) divides \( q_1 \), or \( p_1 \) divides \( q_2 \cdots q_n \). Therefore \( p_1 = q_j \) (for some \( j \)). But by removing \( p_1 \) and \( q_j \) from the initial equivalence we have a smaller integer factorizable in two ways, contradicting our initial assumption. Therefore there can be no such \( s \), and all natural numbers have a unique prime factorization.
Alternate Proof

There exists an alternate, less well known proof that every integer greater than 1 has a unique prime factorization.

Proof of Existence

Take any integer \( n \geq 2 \). If \( n \) is prime, then its prime factorization is itself. If \( n \) is not prime, then it is composite and has two factors greater than one. Factor \( n \) into these two factors, both of which are less than \( n \). Repeat the process until all the factors are prime. This process will not be repeated forever because each new factorization produces positive integers less than previous ones.

Proof of Uniqueness

- Assume the set of all natural numbers that have more than one factorization is non-empty. This set has a least member, according to the Well ordering principle. Call this least member \( k \).
- \( k \) has at least two completely distinct factorizations, \( k = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_n \). If any \( p_i \) equals any \( q_j \) then it can be divided out, and \( k \) isn't the lowest member of the set, so all \( p_i \) are distinct from all \( q_j \). Without loss of generality, assume \( p_1 \leq p_2 \leq p_3 \leq \ldots \leq p_m \) and \( q_1 \leq q_1 \leq q_2 \leq \ldots \leq q_n \). Assume \( p_1 > q_1 \).
- Let \( J = (p_1 - q_1) \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m \). \( J \) is composite and \( J < k \). If \( p_1 - q_1 = r_1 \cdot r_2 \cdot r_3 \cdot \ldots \cdot r_o \) then \( J = r_1 \cdot r_2 \cdot r_3 \cdot \ldots \cdot r_o \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m \), which is one factorization of \( J \).
- But
  \[
  J = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m - q_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_n - q_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m = q_1 \cdot (q_2 \cdot q_3 \cdot \ldots)
  \]
  This means that \( J \) is equal to \( q_1 \cdot s_1 \cdot s_2 \cdot s_3 \cdot \ldots \cdot s_l = (p_1 - q_1) \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m \). \( q_1 \) divides the left side of this equation, but it can't divide the right side because that implies that \( q_1 \) divides \( p_1 \) which can not be. Therefore either \( J \) has two distinct factorizations, in which case let \( W = J \), or one of \( s_k \) equals one of \( r_o \), in which case divide out everything that's equal and let \( W \) equal the remaining primes.
- Either way, \( W \) has two distinct factorizations and \( W < k \), which is a contradiction because \( k \) was the lowest integer that had two factorizations. Therefore, there does not exist an integer \( k \) that has two distinct factorizations, so for all positive integers \( k \) there exists one unique factorization. Q.E.D.

Canonical representation of a positive integer

Since the prime factors of an integer need not be distinct, it follows from the Fundamental Theorem of Arithmetic that each integer \( n > 1 \) can be represented in exactly one way as a product of prime powers (1 corresponding to the empty product)

\[
  n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = \prod_{i=1}^k p_i^{\alpha_i}
\]

where \( p_1 < p_2 < \ldots < p_k \) are primes and the \( \alpha_i \) are positive integers.

This representation is called the canonical representation[4] of \( n \), or the standard form[5] of \( n \).

E.g., \( 12 = 2^2 \cdot 3 \), \( 1296 = 2^4 \cdot 3^4 \), and \( 220 = 2^2 \cdot 5 \cdot 11 \).

If, in a given problem, only one number is represented in this way, we usually require \( \alpha_i \) to be positive for each \( i \), as above. However, for notational convenience when two or more numbers are involved, we sometimes allow some of the exponents to be zero. If \( \alpha_1 = 0 \), for example, the prime \( p_1 \) simply does not occur in the canonical representation of \( n \). This device makes it possible to write the canonical representation of any two positive integers so that they appear to involve the same prime factors even though they may, in fact, fail to have any nontrivial common factor. For example, we could write \( 12 = 2^2 \cdot 3^0 \cdot 5^0 \) and \( 20 = 2^2 \cdot 3^0 \cdot 5^1 \). And one could even write \( 1 = 2^0 \cdot 3^0 \cdot 5^0 \).[6]
This can be taken a bit further: any integer can be uniquely represented as an infinite product taken over all the prime numbers,

\[ n = 2^{n_2}3^{n_3}5^{n_5}7^{n_7} \cdots = \prod p_i^{n_i}, \]

where all but a finite number of the \( n_i \) are zero. (1 corresponding to all \( n_i \) being zero.) This representation is convenient for expressions like these for the product, gcd, and lcm:

\[
\begin{align*}
    a \cdot b &= 2^{a_2+b_2}3^{a_3+b_3}5^{a_5+b_5}7^{a_7+b_7} \cdots = \prod p_i^{a_i+b_i}, \\
    \gcd(a, b) &= 2^{\min(a_2,b_2)}3^{\min(a_3,b_3)}5^{\min(a_5,b_5)}7^{\min(a_7,b_7)} \cdots = \prod p_i^{\min(a_i,b_i)}, \\
    \lcm(a, b) &= 2^{\max(a_2,b_2)}3^{\max(a_3,b_3)}5^{\max(a_5,b_5)}7^{\max(a_7,b_7)} \cdots = \prod p_i^{\max(a_i,b_i)}.
\end{align*}
\]

**Generalizations**

The fundamental theorem of arithmetic generalizes to various contexts; for example in the context of ring theory, where the field of algebraic number theory develops. A ring is said to be a unique factorization domain if the Fundamental theorem of arithmetic (for non-zero elements) holds there. For example, any Euclidean domain or principal ideal domain is necessarily a unique factorization domain. Specifically, a field is trivially a unique factorization domain.

**Notes**

[1] Long (1972, p. 44)  
[3] If \( p_i \) divides \( q_j \) then, since both are prime, \( p_i = q_j \). If, on the other hand, \( p_i \) divides \( q_j - q_x \), then, since \( p_i \) and all \( q_x \) are prime, and we know that \( q_j - q_x \) has a unique prime factorization, then \( p_i \) must be among \( q_j - q_x \).  

**References**

External links

- GCD and the Fundamental Theorem of Arithmetic (http://www.cut-the-knot.org/blue/gcd_fta.shtml) at cut-the-knot
- PlanetMath: Proof of fundamental theorem of arithmetic (http://planetmath.org/encyclopedia/ProofOfFundamentalTheoremOfArithmetic.html)
- Fermat's Last Theorem Blog: Unique Factorization (http://fermatlasttheorem.blogspot.com/2005/06/unique-factorization.html), A blog that covers the history of Fermat's Last Theorem from Diophantus of Alexandria to the proof by Andrew Wiles.