2.3: The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic is one of the most important results in this chapter. It simply says that every positive integer can be written uniquely as a product of primes. The unique factorization is needed to establish much of what comes later. There are systems where unique factorization fails to hold. Many of these examples come from algebraic number theory. We can actually list an easy example where unique factorization fails.

Consider the class \(\{(C)\}\) of positive even integers. Note that \(\{(C)\}\) is closed under multiplication, which means that the product of any two elements in \(\{(C)\}\) is again in \(\{(C)\}\). Suppose now that the only number we know are the members of \(\{(C)\}\). Then we have \(\{(12=2.6)\}\) is composite where as \(\{(14)\}\) is prime since it is not the product of two numbers in \(\{(C)\}\). Now notice that \(\{(60=2.30=6.10)\}\) and thus the factorization is not unique.

We now give examples of the unique factorization of integers.

\[
\begin{align*}
(99 &= 3 \cdot 3 \cdot 11 = 3^2 \cdot 11), \\
(32 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5)
\end{align*}
\]

The Fundamental Theorem of Arithmetic

To prove the fundamental theorem of arithmetic, we need to prove some lemmas about divisibility.

Lemma 4

If \(a,b,c\) are positive integers such that \(\{(a,b)=1\}\) and \(\{(a \mid bc)\}\), then \(\{(a \mid c)\}\).
Since \((a,b)=1\), then there exists integers \((x,y)\) such that \((ax+by=1)\). As a result, \((cax+cby=c)\). Notice that since \((a \mid bc)\), then by Theorem 4, \((a)\) divides \((cax+cby)\) and hence \((a)\) divides \((c)\).

We can generalize the above lemma as such: If \((a,n_i)=1\) for every \((i=1,2,\ldots,n)\) and \((a \mid n_1n_2\ldots n_{k+1})\), then \((a \mid n_{k+1})\). We next prove a case of this generalization and use this to prove the fundamental theorem of arithmetic.

**Lemma 5**

If \((p)\) divides \((n_1n_2n_3\ldots n_k)\), where \(p\) is a prime and \((n_i>0)\) for all \((1 \leq i \leq k)\), then there is an integer \((j)\) with \((1 \leq j \leq k)\) such that \((p \mid n_j)\).

We present the proof of this result by induction. For \((k=1)\), the result is trivial. Assume now that the result is true for \((k)\). Consider \((n_1n_2\ldots n_{k+1})\) that is divisible by \((p)\). Notice that either

\[((p,n_1n_2\ldots n_k)=1  \text{  or  } (p,n_1n_2\ldots n_k)=p.\]

Now if \((p,n_1n_2\ldots n_k)=1\) then by Lemma 4, \((p \mid n_{k+1})\). Now if \((p \mid n_1n_2\ldots n_k)\), then by the induction hypothesis, there exists an integer \((i)\) such that \((p \mid n_i)\).

We now state the fundamental theorem of arithmetic and present the proof using Lemma 5.

**Theorem: The Fundamental Theorem of Arithmetic**

Every positive integer different from 1 can be written uniquely as a product of primes.

If \((n)\) is a prime integer, then \((n)\) itself stands as a product of primes with a single factor. If \((n)\) is composite, we use proof by contradiction. Suppose now that there is some positive integer that cannot be written as the product of primes. Let \((n)\) be the smallest such integer. Let \((n=ab)\), with \((1<a<n)\) and \((1<b<n)\). As a result \((a)\) and \((b)\) are products of primes since both integers are less than \((n)\). As a result, \((n=ab)\) is a product of primes, contradicting that it is not. This shows that every integer can be written as product of primes. We now prove that the representation of a positive integer as a product of primes is unique. Suppose now that there is an integer \((n)\) with two different factorizations say

\[\{n=p_1p_2\ldots p_s=q_1q_2\ldots q_r\}\]

where \((p_1,p_2,\ldots p_s, q_1, q_2, \ldots q_r)\) are primes, \((p_1 \leq p_2 \leq p_3 \leq \ldots \leq p_s)\) \((and)\) \((q_1 \leq q_2 \leq q_3 \leq \ldots \leq q_r)\] Cancel out all common primes from the factorizations above to get

\[\{p_{i_1}p_{i_2}\ldots p_{i_u}=q_{i_1}q_{i_2}\ldots q_{i_v}\}\]

Thus all the primes on the left side are different from the primes on the right side. Since any \((p_{i_1})\) divides \((p_{i_2}\ldots p_{i_u})\), then \((p_{i_1})\) must divide \((q_{i_1}q_{i_2}\ldots q_{i_v})\), and hence by Lemma 5, \((p_{i_1})\) must divide \((q_{i_j})\) for some \((1 \leq k \leq v)\) which is impossible. Hence the representation is unique.
The unique representation of a positive integer \( n \) as a product of primes can be written in several ways. We will present the most common representations. For example, \( n=p_1p_2p_3...p_k \) where \( p_i \) for \( 1 \leq i \leq k \) are not necessarily distinct. Another example would be \( n=p_1^{a_1}p_2^{a_2}p_3^{a_3}...p_j^{a_j} \) where all the \( p_i \) are distinct for \( 1 \leq i \leq j \). One can also write a formal product \( n=\prod_{all \text{ primes }p_i}p_i^{\alpha_i}, \) where all but finitely many of the \( \alpha_i \)'s are 0.

The prime factorization of 120 is given by

\[ 120=2^3\cdot 3\cdot 5. \]

Notice that 120 is written in the two ways described in \[remark1\].

We now describe in general how prime factorization can be used to determine the greatest common divisor of two integers. Let

\[ a=p_1^{a_1}p_2^{a_2}...p_n^{a_n} \quad \text{and} \quad b=p_1^{b_1}p_2^{b_2}...p_n^{b_n}, \]

where we exclude in these expansions any prime \( p_i \) with power 0 in both \( a \) and \( b \) (and thus some of the powers above may be 0 in one expansion but not the other). Of course, if one prime \( p_i \) appears in \( a \) but not in \( b \), then \( a_i \neq 0 \) while \( b_i=0 \), and vice versa. Then the greatest common divisor is given by

\[ (a,b)=p_1^{\min(a_1,b_1)}p_2^{\min(a_2,b_2)}...p_n^{\min(a_n,b_n)}. \]

The following lemma is a consequence of the Fundamental Theorem of Arithmetic.

**Lemma**

Let \( a \) and \( b \) be relatively prime positive integers. Then if \( d \) divides \( ab \), there exists \( d_1 \) and \( d_2 \) such that \( d=d_1d_2 \) where \( d_1 \) is a divisor of \( a \) and \( d_2 \) is a divisor of \( b \). Conversely, if \( d_1 \) and \( d_2 \) are positive divisors of \( a \) and \( b \), respectively, then \( d=d_1d_2 \) is a positive divisor of \( ab \).

Let \( d=\gcd(a,d) \) and \( d=\gcd(b,d) \). Since \( \gcd(a,b)=1 \) and writing \( a \) and \( b \) in terms of their prime decomposition, it is clear that \( d=d_1d_2 \) and \( d=1 \). Note that every prime power in the factorization of \( \gcd(d) \) must appear in either \( d_1 \) or \( d_2 \). Also the prime powers in the factorization of \( \gcd(d) \) that are prime powers dividing \( a \) must appear in \( d_1 \) and that prime powers in the factorization of \( \gcd(d) \) that are prime powers dividing \( b \) must appear in \( d_2 \).

Now conversely, let \( d_1 \) and \( d_2 \) be positive divisors of \( a \) and \( b \), respectively. Then \( d=d_1d_2 \) is a divisor of \( ab \).
More on the Infinitude of Primes

There are also other theorems that discuss the infinitude of primes in a given arithmetic progression. The most famous theorem about primes in arithmetic progression is Dirichlet’s theorem.

Dirichlet’s Theorem

Given an arithmetic progression of terms \( (an+b) \), for \( (n=1, 2, \ldots) \), the series contains an infinite number of primes if \( (a) \) and \( (b) \) are relatively prime.

This result had been conjectured by Gauss but was first proved by Dirichlet. Dirichlet proved this theorem using complex analysis, but the proof is so challenging. As a result, we will present a special case of this theorem and prove that there are infinitely many primes in a given arithmetic progression. Before stating the theorem about the special case of Dirichlet’s theorem, we prove a lemma that will be used in the proof of the mentioned theorem.

If \( (a) \) and \( (b) \) are integers both of the form \( (4n+1) \), then their product \( (ab) \) is of the form \( (4n+1) \)

Let \( (a=4n_1+1) \) and \( (b=4n_2+1) \), then \( (ab=16n_1n_2+4n_1+4n_2+1=4(4n_1n_2+n_1+n_2)+1=4n_3+1) \) where \( (n_3=4n_1n_2+n_1+n_2) \).

There are infinitely many primes of the form \( (4n+3) \), where \( (n) \) is a positive integer.

Suppose that there are finitely many primes of the form \( (4n+3) \), say \( (p_0=3,p_1,p_2,...,p_n) \). Let \( (N=4p_1p_2...p_n+3) \) Notice that any odd prime is of the form \( (4n+1) \) or \( (4n+3) \). Then there is at least one prime in the prime factorization of \( (N) \) of the form \( (4n+3) \), as otherwise, by Lemma 7, \( (N) \) will be in the form \( (4n+1) \). We wish to prove that this prime in the factorization of \( (N) \) is none of \( (p_0=3,p_1,p_2,...,p_n) \). Notice that if \( (3 \mid \text{mid N,}) \) then \( (3 \mid \text{mid (N-3)) and hence [3 \mid \text{mid 4p_1p_2...p_n]} which is impossible since [p_i \text{ ineq 3}) for every [i). Hence 3 doesn’t divide \( (N) \). Also, the other primes \( (p_1,p_2,...,p_n) \) don’t divide \( (N) \) because if \( (p_i \mid \text{mid N}), then \( (p_i \mid \text{mid (N-4p_1p_2...p_n)=3}) \) Hence none of the primes \( (p_0,p_1,p_2,...,p_n) \) divides N. Thus there are infinitely many primes of the form \( (4n+3) \).

Exercises

1. Find the prime factorization of 32, of 800 and of 289.
2. Find the prime factorization of 221122 and of 9!.
3. Show that all the powers of in the prime factorization of an integer \( (a) \) are even if and only if \( a \) is a perfect square.
4. Show that there are infinitely many primes of the form \( (6n+5) \).

Contributors and Attributions

- Dr. Wissam Raji, Ph.D., of the American University in Beirut. His work was selected by the Saylor Foundation’s Open Textbook Challenge for public release under a Creative Commons Attribution (CC BY) license.