5.6: Fundamental Theorem of Arithmetic

Primes are positive integers that do not have any proper divisor except 1. Primes can be regarded as the building blocks of all integers with respect to multiplication.

Theorem \(\PageIndex{1}\): Fundamental Theorem of Arithmetic

Given any integer \(n \geq 2\), there exist primes \(p_1 \leq p_2 \leq \cdots \leq p_s\) such that \(n = p_1 p_2 \cdots p_s\).

Furthermore, this factorization is unique, in the sense that if \(n = q_1 q_2 \cdots q_t\) for some primes \(q_1 \leq q_2 \leq \cdots \leq q_t\), then \(s = t\) and \(p_i = q_i\) for each \(i\), \(1 \leq i \leq s\).

Proof

We first prove the existence of the factorization. Let \(S\) be the set of integers \(n \geq 2\) that are not expressible as the product of primes. Since a product may contain as little as just one prime, \(S\) does not contain any prime. Suppose \(S \neq \emptyset\), then the principle of well-ordering implies that \(S\) has a smallest element \(d\). Since \(S\) does not contain any prime, \(d\) is composite, so \(d = xy\) for some integers \(x\) and \(y\), where \(2 \leq x, y < d\). The minimality of \(d\) implies that \((x, y)\) is not in \(S\). So both \((x, y)\) can be expressed as products of primes, then \(d = xy\) is also a product of primes, which is a contradiction, because \((d, i)\) belongs to \(S\). Therefore, \(S = \emptyset\), which means every integer \(n \geq 2\) can be expressed as a product of primes.

Next, we prove that the factorization is unique. Assume there are two ways to factor \(n\), say \(n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t\). Without loss of generality, we may assume \(s \leq t\). Suppose there exists a smallest \(i\), where \(1 \leq i \leq s\), such that \(p_i \not\mid q_i\). Then \(p_1 = q_1, \quad \text{quad} p_2 = q_2, \quad \text{quad} \cdots \quad \text{quad} p_{i-1} = q_{i-1}, \quad \text{quad} p_i \not\mid q_i\). It follows that \(p_i p_{i+1} \cdots p_s = q_i q_{i+1} \cdots q_t\) in which both sides have at least two factors (why?). Without loss of generality, we may assume \(p_i < q_i\). Since \(p_i \mid q_i q_{i+1}\)
q_t), and (p_i) is prime, Euclid’s lemma implies that (p_i \mid q_j) for some (j), where (i < j \leq t). Since (q_j) is prime, we must have (p_i = q_j \mid q_i), which contradicts the assumption that (p_i < q_i). Therefore, there does not exist any (i) for which (p_i \neq q_i). This means (p_i = q_i) for each (i), and as a consequence, we must have (s = t).

Interestingly, we can use the strong form of induction to prove the existence part of the Fundamental Theorem of Arithmetic.

**Proof**

(Existence) Induct on \( n \). The claim obviously holds for \( n = 2 \). Assume it holds for \( n = 2, 3, \ldots, k \) for some integer \( k \geq 2 \). We want to show that it also holds for \( n = k+1 \). If \( k+1 \) is a prime, we are done. Otherwise, \( k+1 = \alpha \beta \) for some integers \( \alpha \) and \( \beta \), both less than \( k+1 \). Since \( 2 \leq \alpha, \beta \leq k \), both \( \alpha \) and \( \beta \) can be expressed as a product of primes. Putting these primes together, and relabeling and rearranging them if necessary, we see that \( k+1 \) is also expressible as a product of primes in the form we desire. This completes the induction.

The next result is one of the oldest theorems in mathematics, numerous proofs can be found in the literature.

**Theorem** 2

There are infinitely many primes.

**Proof**

Suppose there are only a finite number of primes \( p_1, p_2, \ldots, p_n \). Consider the integer \( x = 1 + p_1 p_2 \cdots p_n \). It is obvious that \( x \neq p_i \) for any \( i \). Since \( p_1, p_2, \ldots, p_n \) are assumed to be the only primes, the integer \( x \) must be composite, hence can be factored into a product of primes. Let \( p_k \) be one of these prime factors, so that \( x = p_k q \) for some integer \( q \). Then \[
\begin{aligned}
x &= 1 + p_1 p_2 \cdots p_n \\
&= q (p_1 p_2 \cdots p_{k-1} p_{k+1} \cdots p_n),
\end{aligned}
\] which is impossible. This contradiction proves that there are infinitely many primes.

Some of the primes listed in the Fundamental Theorem of Arithmetic can be identical. If we group the identical primes together, we obtain the **canonical factorization** or **prime-power factorization** of an integer.

**Theorem** 3

All integers \( n \geq 2 \) can be uniquely expressed in the form \( n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} \) for some distinct primes \( p_i \) and positive integers \( e_i \).

Once we find the prime-power factorization of two integers, their greatest common divisor can be obtained easily.

**Example**

From the factorizations \( 246 = 2 \cdot 3 \cdot 41 \) and \( 426 = 2 \cdot 3 \cdot 79 \), it is clear that \( \gcd(246, 426) = 2 \cdot 3 = 6 \).
hands-on exercise \(\PageIndex{1}\)\label{he:FTA-01}\)

Find the factorizations of 153 and 732, and use them to compute \(\gcd(153,732)\).

Although the set of primes that divide two different positive integers \((a)\) and \((b)\) may be different, we could nevertheless write both \((a)\) and \((b)\) as the product of powers of all the primes involved. For example, by combining the prime factors of \([12300 = 2^2\cdot3\cdot5^2\cdot41, \quad34128 = 2^4\cdot3^3\cdot79,]\) we could write them as \([12300 = 2^2\cdot3^1\cdot5^2\cdot41^1\cdot79^0, \quad34128 = 2^4\cdot3^3\cdot5^0\cdot79^1]\). It follows that \([\gcd(12300,34128) = 2^2\cdot3^1\cdot5^0\cdot41^0\cdot79^0 = 12.]\) The generalization is immediate.

Theorem \(\PageIndex{4}\)

If \(\langle a = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} \rangle \) and \(\langle b = p_1^{f_1} p_2^{f_2} \cdots p_t^{f_t} \rangle \) for some distinct primes \(\langle p_i \rangle\), where \(\langle e_i, f_i \geq 0 \rangle\) for each \(\langle i \rangle\), then \(\langle \gcd(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_t^{\min(e_t,f_t)} \rangle\).

In this theorem, we allow the exponents to be zero. In the usual prime-power factorization, the exponents have to be positive.

hands-on exercise \(\PageIndex{2}\)\label{he:FTA-02}\)

Compute \(\langle \gcd(2^3\cdot5\cdot7\cdot11^2, 2^2\cdot3^2\cdot5^2\cdot7^2) \rangle\).

Definition: least common multiple

The **least common multiple** of the integers \((a)\) and \((b)\), denoted \(\langle \text{ lcm } (a,b) \rangle\), is the smallest positive common multiple of both \((a)\) and \((b)\).

Theorem \(\PageIndex{5}\)

If \(\langle a = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} \rangle \) and \(\langle b = p_1^{f_1} p_2^{f_2} \cdots p_t^{f_t} \rangle \) for some distinct primes \(\langle p_i \rangle\), where \(\langle e_i, f_i \geq 0 \rangle\) for each \(\langle i \rangle\), then \(\langle \text{ lcm } (a,b) = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \cdots p_t^{\max(e_t,f_t)} \rangle\).

hands-on exercise \(\PageIndex{3}\)\label{he:FTA-03}\)

Compute \(\langle \text{ lcm } (2^3\cdot5\cdot7\cdot11^2, 2^2\cdot3^2\cdot5^2\cdot7^2) \rangle\).

Corollary \(\PageIndex{6}\)

For any positive integers \((a)\) and \((b)\), we have \(\langle ab = \gcd(a,b)\cdot\text{ lcm } (a,b) \rangle\).
Proof

For each \( i \), one of the two numbers \( e_i \) and \( f_i \) is the minimum, and the other is the maximum. Hence, \( e_i + f_i = \min(e_i,f_i) + \max(e_i,f_i) \) from which we obtain \( p_i^{e_i} p_i^{f_i} = p_i^{e_i+f_i} = p_i^{\min(e_i,f_i)+\max(f_i,f_i)} = p_i^{\min(e_i,f_i)} p_i^{\max(e_i,f_i)} \). Therefore, \( \gcd(a,b) \) equals the product of \( \gcd(a,b) \) and \( \text{lcm}\{a,b\} \).

Example \( \PageIndex{1} \label{eg:FTA-02} \)

Since \( 12300 = 2^2 \cdot 3^1 \cdot 5^2 \cdot 41^1 \cdot 79^0 \), and \( 34128 = 2^4 \cdot 3^3 \cdot 5^0 \cdot 41^0 \cdot 79^1 \), it follows that \( \gcd(12300,34128) = 2^4 \cdot 3^0 \cdot 5^2 \cdot 41^1 \cdot 79^1 = 34981200 \). We have seen that \( \gcd(12300,34128) = 12 \), and we do have \( 12 \cdot 34981200 = 12300 \cdot 34128 \).

hands-on exercise \( \PageIndex{4} \label{he:FTA-04} \)

Knowing that \( \gcd(246,426) = 6 \), how would you compute the value of \( \text{lcm}\{246,426\} \)?

Example \( \PageIndex{3} \label{eg:FTA-03} \)

When we add two fractions, we first take the common denominator, as in \( \frac{7}{8} + \frac{5}{12} = \frac{7}{8} \cdot \frac{3}{3} + \frac{5}{12} \cdot \frac{2}{2} = \frac{21+10}{24} = \frac{31}{24} \). Clear enough, the least common denominator is precisely the least common multiple of the two denominators.

Example \( \PageIndex{4} \label{eg:FTA-04} \)

The control panel of a machine has two signal lights, one red and one blue. The red light blinks once every 10 seconds, and the blue light blinks once every 14 seconds. When the machine is turned on, both lights blink simultaneously. After how many seconds will they blink at the same time again?

Solution

This problem illustrates a typical application of least common multiple. The red light blinks at 10, 20, 30, … seconds, while the blue light blinks at 14, 28, 42, … seconds. In general, the red light blinks at \( t \) seconds if \( t \) is a multiple of 10, and the blue light blinks when \( t \) is a multiple of 14. Therefore, both lights blink together when \( t \) is a multiple of both 10 and 14. The next time it happens will be \( \text{lcm}\{10,14\} = 70 \) seconds later.

hands-on exercise \( \PageIndex{5} \label{he:FTA-05} \)

Two comets travel on fixed orbits around the earth. One of them returns to Earth every 35 years, the other every 42 years. If they both appear in 2012, when is the next time they will return to Earth in the same year?

hands-on exercise \( \PageIndex{6} \label{he:FTA-06} \)

Given relatively prime positive integers \( m \) and \( n \), what are the possible values of \( \text{lcm}\{4m-6n,6m+4n\} \)?
Example \(\PageIndex{5}\)\label{eg:FTA-05}\)

What does \(2\mathbb{Z}\cap3\mathbb{Z}\) equal to?

**Solution**

Assume \(x\in 2\mathbb{Z}\cap3\mathbb{Z}\), then \(x\in 2\mathbb{Z}\) and \(x\in 3\mathbb{Z}\). This means \(x\) is a multiple of both 2 and 3. Consequently, \(x\) is a multiple of \(\text{lcm}(2,3)=6\), which means \(x\in 6\mathbb{Z}\). Therefore, \(2\mathbb{Z}\cap3\mathbb{Z}\subseteq 6\mathbb{Z}\).

Next, assume \(x\in 6\mathbb{Z}\), then \(x\) is a multiple of 6. Consequently, \(x\) is a multiple of 2, as well as a multiple of 3. This means \(x\in 2\mathbb{Z}\) and \(x\in 3\mathbb{Z}\). As a result, \(x\in 2\mathbb{Z}\cap3\mathbb{Z}\). Therefore, \(6\mathbb{Z}\subseteq 2\mathbb{Z}\cap3\mathbb{Z}\). Together with \(2\mathbb{Z}\cap3\mathbb{Z}\subseteq 6\mathbb{Z}\), we conclude that \(2\mathbb{Z}\cap3\mathbb{Z}=6\mathbb{Z}\).

hands-on exercise \(\PageIndex{7}\)\label{he:FTA-07}\)

What does \(4\mathbb{Z}\cap6\mathbb{Z}\) equal to?

---

**Summary and Review**

- There are infinitely many primes.
- Any positive integer \(n>1\) can be uniquely factored into a product of prime powers.
- Primes can be considered as the building blocks (through multiplication) of all positive integers exceeding one.
- Given two positive integers \(a\) and \(b\), their least common multiple is denoted as \(\text{lcm}(a,b)\).
- For any positive integers \(a\) and \(b\), we have \(ab = \gcd(a,b)\cdot\text{lcm}(a,b)\).

Exercise \(\PageIndex{1}\)\label{ex:FTA-01}\)

Find the prime-power factorization of these integers.

1.25 (a) 4725 & (b) 9702
   (c) 18065 & (d) 1662405

Exercise \(\PageIndex{2}\)\label{ex:FTA-02}\)

Find the least common multiple of each of the following pairs of integers.

1.25 (a) 27, 81 & (b) 24, 84 & (c) 120, 615
   (d) 412, 936 & (e) 1380, 3020 & (f) 1122, 3672

Exercise \(\PageIndex{3}\)\label{ex:FTA-03}\)

Richard follows a very rigid routine. He orders a pizza for lunch every 10 days, and has dinner with his parents every 25 days.
If he orders a pizza for lunch and has dinner with his parents today, when will he do both on the same day again?

Exercise \(\PageIndex{4}\) \label{ex:FTA-04}\)

Compute \(\gcd(15\cdot50,25\cdot21)\), and \(\lcm (15\cdot25,21)\).

Exercise \(\PageIndex{5}\) \label{ex:FTA-05}\)

What does \(10\mathbb{Z}\cap 15\mathbb{Z}\) equal to? Prove your claim.

Exercise \(\PageIndex{6}\) \label{ex:FTA-06}\)

Let \(\langle m\rangle\) and \(\langle n\rangle\) be positive integers. What does \(\langle m\rangle\cap \langle n\rangle\) equal to? Prove your claim.

Exercise \(\PageIndex{7}\) \label{ex:FTA-07}\)

Let \(\langle p\rangle\) be an odd prime. Show that

- \(\langle p\rangle\) is of the form \(4k+1\) or of the form \(4k+3\) for some nonnegative integer \(k\).
- \(\langle p\rangle\) is of the form \(6k+1\) or of the form \(6k+5\) for some nonnegative integer \(k\).

Exercise \(\PageIndex{8}\) \label{ex:FTA-08}\)

Give three examples of an odd prime \(\langle p\rangle\) of each of the following forms

1.25 (a) \(4k+1\) & (b) \(4k+3\)
(c) \(6k+1\) & (d) \(6k+5\)

Exercise \(\PageIndex{9}\) \label{ex:FTA-09}\)

Prove that any prime of the form \(3n+1\) is also of the form \(6k+1\).

Exercise \(\PageIndex{10}\) \label{ex:FTA-10}\)

Prove that if a positive integer \(\langle n\rangle\) is of the form \(3k+2\), then it has a prime factor of the same form.

**Hint**

Consider its contrapositive.

Exercise \(\PageIndex{11}\) \label{ex:FTA-11}\)

Prove that 5 is the only prime of the form \(n^2-4\).

**Hint**

Consider the factorization of \(n^2-4\).
Exercise \(\PageIndex{12}\)\label{ex:FTA-12}\)

Use the result “Any odd prime \(p\) is of the form \(6k+1\) or of the form \(6k+5\) for some nonnegative integer \(k\)” to prove the following results.

- If \(p\geq5\) is a prime, then \(p^2+2\) is composite.
- If \(p\geq q\geq5\) are primes, then \(24\mid(p^2-q^2)\).