DEFINITION 1 An integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite*.

EXAMPLE 1.1 Determine if 7 is prime.
Solution: The only integers that divide 7 are 1 and 7 and, by definition 1, 7 is prime.

EXAMPLE 1.2 Determine if 9 is prime.
Solution: $3|9$ and, therefore, 9 is not prime but composite.

THEOREM 1 **THE FUNDAMENTAL THEOREM OF ARITHMETIC**. Every positive integer greater than 1 can be written uniquely as a prime or the product of two or more primes where the prime factors are written in order of nondecreasing size.

EXAMPLE 2.1 Find the prime factorization of 100.
Solution: $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

EXAMPLE 2.2 Find the prime factorization of 641.
Solution: $641 = 641$.

EXAMPLE 2.3 Find the prime factorization of 999.
Solution: $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$

EXAMPLE 2.4 Find the prime factorization of 1024.
Solution: $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Trial Division

THEOREM 2 If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

EXAMPLE 3 Show that 101 is prime.
Solution: If we can find no prime factors of 101 less than $\sqrt{101}$ then 101 is prime.

- $2 \nmid 101$
- $3 \nmid 101$
- $5 \nmid 101$
- $7 \nmid 101$

Hence, 101 is prime.

EXAMPLE 4 Find the prime factorization of 7007

Solution: Factors of 7007 must be less than or equal to $\sqrt{7007} = 83$.

$$7007 = 7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$$

The Sieve of Eratosthenes

Note that composite integers not exceeding 100 must have a prime factor not exceeding 10. Because the only primes less than 10 are 2, 3, 5, and 7, the primes not exceeding 100 are these four primes and those positive integers greater than 1 and not exceeding 100 that are divisible by none of 2, 3, 5, or 7.

The **sieve of Eratosthenes** is used to find all primes not exceeding a specified positive integer. For instance, the following procedure is used to find the primes not exceeding 100. We begin with the list of all integers between 1 and 100. To begin the sieving process, the integers that are divisible by 2, other than 2, are deleted. Because 3 is the first integer greater that 2 that is left, all those integers divisible by 3, other than 3, are deleted. We continue finding primes and deleting their multiples until we have reached the square root of the maximum value. In this case the $\sqrt{100} = 10$. The remaining integers are prime.

Original									
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Remove multiples of 2 but not 2 itself.									
1	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	

Remove multiples of 3 but not 3 itself.									
1	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83		85				89	
91				95		97			

Remove multiples of 5 but not 5 itself.									
1	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			

Remove multiples of 7 but not 7 itself.									
1	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

THEOREM 3 There are infinitely many primes.

Remark A Mersenne prime has the form $2^p - 1$ where p is prime. Not all values of the form $2^p - 1$ are prime but there exists an efficient test, known as the Lucas-Lehmer test, for determining whether $2^p - 1$ is prime.

EXAMPLE 5 Find the first value of the form $2^p - 1$ that is not prime.

Solution:

Prime	$2^p - 1$	Is it a prime number
2	$2^2 - 1 = 3$	yes
3	$2^3 - 1 = 7$	yes
5	$2^5 - 1 = 31$	yes
7	$2^7 - 1 = 127$	yes
11	$2^{11} - 1 = 2047 = 23 \cdot 89$	no

THEOREM 4 **THE PRIME NUMBER THEOREM**. The ratio of the number of primes not exceeding x and $x/\ln x$ approaches 1 as x grows without bound. (Here $\ln x$ is the natural logarithm of x.)

Greatest Common Divisors and Least Common Multiples

DEFINITION 2 Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by gcd(a,b).

EXAMPLE 10 What is the greatest common divisor of 24 and 36?

Solution:

Dividend	Divisors
24	1, 2, 3, 4, 6, 8, 12, 24
36	1, 2, 3, 4, 6, 9, 12, 18, 36

The gcd(24,36)=12

EXAMPLE 11 What is the greatest common divisor of 17 and 22?

Solution:

Dividend	Divisors
17	1, 17
22	1, 2, 11, 22

The gcd(17,22)=1

DEFINITION 3 The integers a and b are relatively prime if their greatest common divisor is 1.

EXAMPLE 12 Are 17 and 22 relatively prime?

Solution: Yes, because gcd(17,22)=1

DEFINITION 4 The integers $a_1, a_2, \cdots, a_n$ are pairwise relatively prime if gcd(a_i, a_j)=1 whenever $1 \leq i < j \leq n$

EXAMPLE 13.1 Determine whether the integers 10, 17, and 21 are pairwise relatively prime.

Solution:

Dividend	**Divisors**
10	1, 2, 5, 10
17	1, 17
21	1, 3, 7, 21

Pair		**gcd**	
10	17	1	Relatively prime
10	21	1	Relatively prime
17	21	1	Relatively prime

EXAMPLE 13.2 Determine whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution:

Dividend	**Divisors**
10	1, 2, 5, 10
19	1, 19
24	1, 2, 3, 4, 6, 8, 12, 24

Pair		**gcd**	
10	19	1	Relatively prime
10	24	2	Not relatively prime
19	24	1	Relatively prime

Prime factorization method of finding the greatest common divisor:

1. Find the prime factorization of both integers.
2. Identify common prime factors
3. Identify the minimum exponent common to both factorizations on common prime factors.
4. Find the product of those factors found in step 3.

EXAMPLE 14 What is the greatest common divisor of 120 and 500?

Solution:

Integer	**Prime factorization**
120	$2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5$
500	$2 \cdot 2 \cdot 5 \cdot 5 \cdot 5 = 2^2 \cdot 5^3$
Common Factors	
2^2	
5	
gcd	
20	

DEFINITION 5 The *least common multiple* of the positive integers a and b is the smallest ***positive*** integer that is divisible by both a and b. The least common multiple of a and b is denoted by lcm(a,b).

Prime factorization method for finding the least common multiple of a and b.

1. Find the prime factorization of a.
2. Find the prime factorization of b.

3. For every prime in the factorizations of both a and b, find the **largest** exponent.
4. The least common multiple is product of the list generated in step 3.

EXAMPLE 15 What is the least common multiple of 95,256 and 432?

Solution:

Integer	Prime factorization
95,256	$2^3 \cdot 3^5 \cdot 7^2$
432	$2^4 \cdot 3^3$
Maximum Factors	
2^4	
3^5	
7^2	
lcm	
$2^4 \cdot 3^5 \cdot 7^2$	

THEOREM 5 Let a and b be positive integers. Then

$$ab = \gcd(a, b) \cdot \text{lcm}(a, b)$$