# Lecture 16

Topics:

1. Prime Numbers
2. Prime Factorization
3. Relative Prime Number
4. Fermat's Little Theorem

# 4.3.2 Primes

**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** The integer 7 is prime because it's only positive factors are 1 and 7, whereas the integer 9 is composite because it is divisible by 3.

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

# EXAMPLE 2

The prime factorizations of 100, 641, 999, and 1024 are given by:

$100 = 2 * 2 * 5 * 5 = 2^2 5^2$,

$641 = 641$ ,

$999 = 3 * 3 * 3 * 37 = 3^3 \cdot 37$,

$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$.

# THEOREM 2

If n is a composite integer, then n has a prime divisor less than or equal to √n.
**Proof:** If n is composite, by the definition of a composite integer, we know that it has a factor “a” with **1 < a < n.** Hence, by the definition of a factor of a positive integer, we have **n = a*b**, where b is a positive integer greater than 1. We will show that **a ≤ √n** or **b ≤ √n**. If **a > √n** and **b > √n,** then **a*b > √n** ·

**√n = n**, which is a contradiction. Consequently, **a ≤ √n** or **b ≤ √n.** Because both a and b are divisors of n, we see that n has a positive divisor not exceeding **√n.** This divisor is either prime or, by the fundamental theorem of arithmetic, has a prime divisor less than itself. In either case, n has a prime divisor less than or equal to **√n.**

**Example 3: Show that 101 is prime.**

**Solution:** The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer), it follows that 101 is prime.

**EXAMPLE 4: Find the prime factorization of 7007.**

**Solution:** To find the prime factorization of 7007, first perform divisions of 7007 by successive primes, beginning with 2. None of the primes 2, 3, and 5 divides 7007. However, 7 divides 7007, with $7007/7 = 1001$.

Next, divide 1001 by successive primes, beginning with 7. It is immediately seen that 7 also divides 1001, because $1001/7 = 143$. Continue by dividing 143 by successive primes, beginning with 7. Although 7 does not divide 143, 11 does divide 143, and $143/11 = 13$. Because 13 is prime, the procedure is completed. It follows that

$7007 = 7 * 1001 = 7 * 7 * 143 = 7 * 7 * 11 * 13$

Consequently, the prime factorization of 7007 is $7 * 7 * 11 * 13 = 7^2 * 11 * 13$.

# THEOREM 3 There are infinitely many primes.

**Proof:** We will prove this theorem using a proof by contradiction. We assume that there are only finitely many primes, $\mathbf{p_1, p_2, \dots, p_n}$.

**Let $\mathbf{Q = p_1 , p_2 \dots \ p_n + 1.}$** By the fundamental theorem of arithmetic, Q is prime or else it can be written as the product of two or more primes. However, none of the primes $p_j$ divides Q, for if $p_j \mid Q$, then $p_j$ divides $\mathbf{Q - p_1 p_2 \dots \ p_n = 1.}$ Hence, there is a prime not in the list $\mathbf{p_1, p_2, \dots, p_n}$. This prime is either Q, if it is prime, or a prime factor of Q. This is a contradiction because we assumed that we have listed all the primes.

Consequently, there are infinitely many primes.

Self Study

# 4.3.5 Conjectures and Open Problems About Primes

**EXAMPLE 6** It would be useful to have a function f(n) such that f(n) is prime for all positive integers n. If we Extra had such a function, we could find large primes for use in cryptography and other applications.

Examples Looking for such a function, we might check out different polynomial functions, as some mathematicians did several hundred years ago. After a lot of computation we may encounter the polynomial

$f(n) = n^2 - n + 41$. This polynomial has the interesting property that f(n) is prime for all positive integers n not exceeding 40. [We have f(1) = 41, f(2) = 43, f(3) = 47,f(4) = 53, and so on.]

This can lead us to the conjecture that f(n) is prime for all positive integers n.

Self Study

EXAMPLE 7: Goldbach's Conjecture In 1742, Christian Goldbach, in a letter to Leonhard Euler, conjectured that every odd integer n, $n > 5$, is the sum of three primes. Euler replied that this conjecture is equivalent to the conjecture that every even integer n, $n > 2$, is the sum of two primes (see Exercise 21 in the Supplementary Exercises). The conjecture that every even integer n, $n > 2$, is the sum of two primes is now called Goldbach's conjecture. We can check this conjecture

for small even numbers. **For example, 4 = 2 + 2, 6 = 3 + 3, 8 = 5 + 3, 10 = 7 + 3, 12 = 7 + 5,**

and so on. Goldbach's conjecture was verified by hand calculations for numbers up to the advent of computers. With computers it can be checked for extremely large numbers. As of early 2018, the conjecture has been checked for all positive even integers up to $4 \cdot 10^{18}$.

**EXAMPLE 9** The Twin Prime Conjecture Twin primes are pairs of primes that differ by 2, such as 3 and 5, 5 and 7, 11 and 13, 17 and 19, and 4967 and 4969. The twin prime conjecture asserts that there are infinitely many twin primes. The strongest result proved concerning twin primes is that Links there are infinitely many pairs p and p + 2, where p is prime and p + 2 is prime or the product of two primes (proved by J. R. Chen in 1966).

# 4.3.6 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:** The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12.

Hence, **gcd(24, 36) = 12.**

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

**Definition 4** The integers $\mathbf{a_1, a_2, \ldots, a_n}$ are pairwise relatively prime i**f** $\mathbf{gcd(a_i, a_j) = 1}$ whenever $\mathbf{1 \leq i < j \leq n}$.

**EXAMPLE 13** Determine whether the integers 10, 17, and 21 are pairwise relatively prime and whether the integers 10, 19, and 24 are pairwise relatively prime.

**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).

**THEOREM 5** Let a and b be positive integers.

Then a * b = gcd(a, b) * lcm(a, b).

**THEOREM 1** If a and m are relatively prime integers and **m > 1**, then an inverse of a modulo m exists.

Furthermore, this inverse is unique modulo m. (That is, there is a unique positive integer a less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to a modulo m.)

Proof: By Theorem 6 of Section 4.3, because gcd(a, m) = 1, there are integers s and t such that

$s * a + t * m = 1$.

This implies that $s * a + t * m \equiv 1 \pmod{m}$.

Because $t * m \equiv 0 \pmod{m}$, it follows that

$s * a \equiv 1 \pmod{m}$.

# 4.4.5 Fermat's Little Theorem

**THEOREM 3 FERMAT'S LITTLE THEOREM** If p is prime and a is an integer not divisible by p, then $\mathbf{a^{p-1} \equiv 1 \pmod{p}}$. Furthermore, for every integer a we have $\mathbf{a^p \equiv a \pmod{p}}$.

**EXAMPLE 9** Find $\mathbf{7^{222} \bmod 11}$.

**Solution:** We can use Fermat's little theorem to evaluate $\mathbf{7^{222} \bmod 11}$ rather than using the fast modular exponentiation algorithm. By Fermat's little theorem we know that $\mathbf{7^{10} \equiv 1 \pmod{11}}$, so $\mathbf{(7^{10})^k \equiv 1 \pmod{11}}$ for every positive integer k. To take advantage of this last congruence, we divide the exponent 222 by 10, finding that $\mathbf{222 = 22 \cdot 10 + 2}$.

We now see that $\mathbf{7^{222} = 7^{22 \cdot 10+2} = (7^{10})}$

$7^{222} \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}$. It follows that $7^{222} \bmod 11 = 5$.

# End of Lecture 16