When the modulo of two integers are equal

In modular arithmetic, it is the divisor that, once divided as many times as it can into the divisor, will result in the remainder of the division

The set of all integers congruent to an integer a modulo m

The set of nonnegative integers less than m

Used when performing tasks utilizing the operations +m and @u2022m

Let b be an integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form [ n = a@u2093b^x + a@u2093@u208b@u2081b^(x-1)+...+a@u2081b+a@u2080 [ Where x is a nonnegative integer, a@u2080, a@u2081, ..., a@u2093 are nonnegative integers less than b, and a@u2093 ≠ 0

base 10 expansion of integers

base 2 expansion of integers

base 8 expansion of integers

base 16 expansion of integers

bit strings of length 8

Positive integers that have exactly two different positive integer factors

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

A brute-force algorithm that divides some integer n by all primes not exceeding √n and concludes that n is prime if it is not divisible by any of these primes

An algorithm that finds the greatest common divisor of two integers by using successive division to reduce the problem to two smaller integers until one of the integers is zero

For two integers a and b, there exists integers s and t such that the greatest common divisor between a and b can be expressed as gcd(a, b) = sa + tb

A method of finding the linear combination of two integers’ greatest common divisor by making a forward pass through the Euclidean algorithm and then making a backward pass through its steps in order to the integers s and t when constructing the linear combination

Numbers generated by systematic methods

The process of making a message secret

The process of determining the original message from an encrypted message