**GCD-**

The greatest common divisor (GCD) is a fundamental concept in number theory that represents the largest positive integer that divides two or more given integers without leaving a remainder. It is also known as the greatest common factor (GCF) or highest common factor (HCF).

The GCD of two integers "a" and "b" is denoted as GCD(a, b). It has several important properties:

1. Divisibility: The GCD(a, b) divides both "a" and "b" without leaving a remainder. In other words, "a" and "b" are both divisible by GCD(a, b).
2. Common Divisors: GCD(a, b) is the largest positive integer that divides both "a" and "b". Any other common divisor of "a" and "b" is necessarily smaller than or equal to GCD(a, b).
3. Relatively Prime: If GCD(a, b) = 1, "a" and "b" are said to be relatively prime or coprime. It means that "a" and "b" have no common factors other than 1. Relatively prime numbers have a GCD of 1.
4. GCD and Prime Factors: The GCD of two numbers can be computed based on their prime factorization. If "a" has prime factors p1^a1 \* p2^a2 \* ... \* pn^an, and "b" has prime factors q1^b1 \* q2^b2 \* ... \* qm^bm, then the GCD(a, b) is equal to p1^min(a1, b1) \* p2^min(a2, b2) \* ... \* pn^min(an, bn), where min(a, b) represents the minimum of "a" and "b".
5. Euclidean Algorithm: The Euclidean algorithm is a widely used method to compute the GCD of two numbers efficiently. It involves repeatedly replacing the larger number with the remainder obtained from dividing the larger number by the smaller number, until the remainder becomes zero. The GCD is then the non-zero remainder obtained in the previous step. The Euclidean algorithm is based on the observation that the GCD of two numbers remains the same if the larger number is replaced by its remainder when divided by the smaller number.

The GCD has numerous applications in number theory and cryptography. It forms the basis of various algorithms and techniques, including reducing fractions to their simplest form, modular arithmetic operations, primality testing, and key generation in public-key cryptography systems like RSA. The ability to compute the GCD efficiently is crucial in many computational tasks involving integers.