One of the fundamental techniques used in cryptography is the Extended Euclidean Algorithm, which is used to compute the greatest common divisor of two integers. It is also used to find the coefficients, which can be used to express the GCD as a line using two seperate integers. The Extended Euclidean Algorithm is useful in cryptography and number theory, to find these exact values. The algorithm is relatively simple to implement in practice.

History

The Extended Euclidean Algorithm is named after the ancient Greek mathematician Euclid, who first described the Euclidean Algorithm for finding the GCD of two integers. The Extended Euclidean Algorithm is an extension of this algorithm and this prehistoric mathematician. The algorithm was used in modular arithmetic, which is used in cryptography. In modern times, the algorithm is wildly used.

Encryption Process

The Extended Euclidean Algorithm can be used in encryption by generating a public and private key pair. To encrypt a message, the sender uses the public key to generate a ciphertext, which can only be decrypted using the private key. The algorithm's advantage is that it can generate large prime numbers quickly.

Here is an example of how to use the Extended Euclidean Algorithm, with much smaller values than what would be used, to find the GCD and coefficients of Bezout's identity

Numbers = 54 and 24.

We start by setting up the algorithm as follows:

Let a = 54 and b = 24

We want to find the GCD of a and b and the coefficients x and y in Bezout's identity such that ax + by = GCD(a,b).

Next, we use the following steps to calculate the GCD and the coefficients:

Step 1: Divide a by b and find the remainder:

54 = 2 × 24 + 6

Step 2: Divide b by the remainder and find the new remainder:

24 = 4 × 6 + 0

Step 3: Express the remainder (6) as a linear combination of a and b:

6 = 54 - 2 × 24

Step 4: Substitute the remainder into the equation and repeat:

6 = 54 - 2 × (24)

6 = 54 - 2 × (54 - 2 × 24)

6 = 5 × 54 - 2 × 24

Step 5: The GCD of a and b is the final remainder, which in this case is 6. The coefficients of Bezout's identity are the coefficients of a and b in the final equation, which is 5 and -2, respectively. Therefore, the GCD of 54 and 24 is 6, and we can express 6 as 5 × 54 - 2 × 24.

Security

The Extended Euclidean Algorithm is considered to be secure, due to how hard factoring large numbers into their prime factors can be. However, the security of the algorithm can be compromised if the parameters used in the algorithm are not chosen correctly. For example, if the two integers used in the algorithm have a small difference, an attacker may be able to factor in the integers and derive the private key (like above). Using a large prime numbers and ensuring that the parameters are chosen randomly is needed for the algorithm's security.