Copilot

The **extended Euclidean algorithm** is an extension of the regular Euclidean algorithm. It serves two purposes: finding the greatest common divisor (GCD) of two integers and computing the coefficients of Bézout's identity. Let's break it down:

1. **Greatest Common Divisor (GCD)**:
    - The Euclidean algorithm is used to compute the GCD of two integers. It repeatedly divides the larger number by the smaller number until the remainder becomes zero. The GCD is the last non-zero remainder.
    - For example, consider finding the GCD of 102 and 38: [\begin{aligned} 102 &= 2 \times 38 + 26 \ 38 &= 1 \times 26 + 12 \ 26 &= 2 \times 12 + 2 \ 12 &= 6 \times 2 + 0. \end{aligned}] The GCD is 2 because it's the last non-zero remainder before the algorithm terminates.

2. **Extended Euclidean Algorithm**:
    - Given two integers (a) and (b), the extended Euclidean algorithm computes integers (x) and (y) such that (ax + by = \gcd(a, b)).
    - Bézout's lemma guarantees the existence of such integers.
    - The algorithm reverses the steps of the Euclidean algorithm to find (x) and (y). We start with the GCD and recursively work our way backward.
    - For example, let's find (x) and (y) for 102 and 38:
        - Start with the GCD: (2 = 26 - 2 \times 12).
        - Replace 12 using the previous line: (2 = 26 - 2 \times (38 - 1 \times 26)).
        - Collect like terms: (2 = 3 \times 26 - 2 \times 38).
        - Repeat the process until we get the final result: (2 = 3 \times 102 - 8 \times 38).

The extended Euclidean algorithm is also useful for solving Diophantine equations and finding modular inverses efficiently. If you have any specific questions or need further clarification, feel free to ask!