

DS

Extended Euclidean Algorithm to find multiplicative inverse.


The Extended Euclidean Algorithm is an algorithm to find the multiplicative inverse of two numbers in modular arithmetic. It is a generalization of the Euclidean algorithm for finding the greatest common divisor. Given two numbers a and b (with b being the modulus), the algorithm finds integers x and y such that $ax \equiv 1 \pmod{b}$. In other words, x is the multiplicative inverse of a modulo b if $ax \equiv 1 \pmod{b}$. If $\gcd(a, b) \neq 1$, then a doesn't have a multiplicative inverse modulo b .



DS

Give a example js function to implement that without using any inbuilt function.


Here's an example implementation of the Extended Euclidean Algorithm in JavaScript to find the multiplicative inverse of a modulo b :

css

Copy code

```
function extendedEuclidean(a, b) {
  let x = 1, y = 0;
  let xLast = 0, yLast = 1;
  let q, r, m, n;
  while (b !== 0) {
    q = Math.floor(a / b);
    r = a % b;
    m = xLast - q * x;
    n = yLast - q * y;
    xLast = x; yLast = y;
    x = m; y = n;
    a = b; b = r;
  }
  return {a: a, x: xLast, y: yLast};
}

function inverseModulo(a, b) {
  let result = extendedEuclidean(a, b);
  if (result.a !== 1) return NaN;
  let inverse = (result.x % b + b) % b;
  return inverse;
}
```

You can use this function `inverseModulo(a, b)` to find the multiplicative inverse of a modulo b . If $\gcd(a, b) \neq 1$, the function returns `NaN`.



DS

What is extended euclidean algorithm


The Extended Euclidean Algorithm is an algorithm that finds the greatest common divisor (GCD) of two numbers and also finds the coefficients x and y such that $ax + by = \gcd(a, b)$, where $\gcd(a, b)$ is the GCD of a and b . In addition to finding the GCD, the Extended Euclidean Algorithm can also be used to solve modular linear equations, such as finding the modular inverse of a number, and to solve Diophantine equations, which are equations with integer solutions. The algorithm is an extension of the classical Euclidean Algorithm for finding the GCD of two numbers.