Aim: - To Understand the Extended Euclidian Algorithm.

Objective: - To implement Extended Euclidian Algorithm using BigIntegers in Java. But not to use the library method of java.

Explanation of Extended Euclidian Algorithm.

Extended Euclidian Algorithm is an extension to Euclidian Algorithm, which computes the Greatest Common Divisor but also helps to find Bezout’s Identity. Consider the following: -

, Then there exists two numbers a and b such that

The Algorithm helps us to find these coefficients ‘*a’* and ‘*b’ .* We calculate the as same as we do with Euclidian Algorithm. Then to get the linear combination we just multiply the values diagonally as show in the table below:-

|  |  |  |
| --- | --- | --- |
| a | q | y |
| 246 | - | 52 |
| 194 | 1 | 41 |
| 52 | 3 | 11 |
| 38 | 1 | 8 |
| 14 | 2 | 3 |
| 10 | 1 | 2 |
| 4 | 2 | 1 |
| 2 | 2 | 0 |

Thus

The a and q columns are filled in using the Euclidean algorithm, i.e. by successive division: Divide the next-to-the-last a by the last a. The quotient goes into the q-column, and the remainder goes into the a-column. And at last by taking the numbers diagonally, we get the linear combination.

Now why this algorithm works (Mathematically)

As it helps us to find Bezout’s Identity,

So Bezout’s Identity says that:- For any positive integers , there exists

Q3 What are the uses of Euclidian Algorithm.

The uses/applications of Euclidian algorithm are as follows:-

* Bézout's identity
* Linear Diophantine equations.
* Chinese remainder Theorem.(Multiple Linear Diophantine Equations).
* Factorization Algorithms.

Screenshots of the working program:-

Given the two inputs x and y the program outputs as follows:-

