SurajSG23 Create Extended Euclidean Algorithm b107d92 · now

66 lines (50 loc) · 1.77 KB

Code Blame Raw

```java
import java.util.Scanner;

public class ExtendedEuclidean {

    // Extended Euclidean Algorithm to find gcd and coefficients x, y
    public static int[] extendedEuclid(int a, int m) {
        if (m == 0) {
            return new int[] { a, 1, 0 };
        }

        int[] result = extendedEuclid(m, a % m);
        int gcd = result[0];
        int x1 = result[1];
        int y1 = result[2];

        // Update x and y using the recursive results
        int x = y1;
        int y = x1 - (a / m) * y1;

        return new int[] { gcd, x, y };
    }

    // Function to find the modular inverse of a mod m
    public static int modInverse(int a, int m) {
        int[] result = extendedEuclid(a, m);
        int gcd = result[0];
        int x = result[1];

        // If gcd(a, m) is not 1, then the inverse does not exist
        if (gcd != 1) {
            return -1; // No modular inverse exists
        } else {
            // Ensure x is positive and return it as the modular inverse
            return (x % m + m) % m;
        }
    }
```

```
37
38          public static void main(String[] args) {
39              Scanner scanner = new Scanner(System.in);
40
41              // Take input from the user
42              System.out.print("Enter a number (a): ");
43              int a = scanner.nextInt();
44
45              int m = 26; // Number of letters in the alphabet
46
47              // Calculate modular inverse
48              int inverse = modInverse(a, m);
49
50              if (inverse == -1) {
51                  System.out.println("No modular inverse exists for " + a + " modulo "
52              } else {
53                  System.out.println("The modular inverse of " + a + " modulo " + m +
54              }
55
56              scanner.close();
57          }
58      }
59
60      //Output
61
62      Enter a number (a): 5
63      The modular inverse of 5 modulo 26 is: 21
64
65      Enter a number (a): 13
66      No modular inverse exists for 13 modulo 26
```