Extended Euclidean Algorithm

Table of Contents

While the Euclidean algorithm calculates only the greatest common divisor (GCD) of two integers a and b, the extended version also finds a way to represent GCD in terms of a and b, i.e. coefficients x and y for which:

$$a \cdot x + b \cdot y = \gcd(a, b)$$

Algorithm

The changes to the original algorithm are very simple. All we need to do is to figure out how the coefficients x and y change during the transition from (a, b) to $(b \bmod a, a)$.

Let us assume we found the coefficients (x_1, y_1) for $(b \bmod a, a)$:

$$(b \bmod a) \cdot x_1 + a \cdot y_1 = g$$

and we want to find the pair (x, y) for (a, b):

$$a \cdot x + b \cdot y = g$$

We can represent $b \bmod a$ is:

$$b \bmod a = b - \left\lfloor \frac{b}{a} \right\rfloor \cdot a$$

Substituting this expression in the coefficient equation of (x_1, y_1) gives:

$$g = (b \bmod a) \cdot x_1 + a \cdot y_1 = \left(b - \left\lfloor \frac{b}{a} \right\rfloor \cdot a \right) \cdot x_1 + a \cdot$$

and after rearranging the terms:

$$g = b \cdot x_1 + a \cdot \left(y_1 - \left\lfloor \frac{b}{a} \right\rfloor \cdot x_1 \right)$$

We found the values of x and y:

$$\begin{cases} x = y_1 - \left\lfloor \frac{b}{a} \right\rfloor \cdot x_1 \\ y = x_1 \end{cases}$$

Implementation

```
int gcd(int a, int b, int & x, int & y) {
    if (a == 0) {
        x = 0;
        y = 1;
        return b;
    }
    int x1, y1;
    int d = gcd(b % a, a, x1, y1);
    x = y1 - (b / a) * x1;
    y = x1;
    return d;
}
```

The recursive function above returns the GCD and the values of coefficients to `x` and `y` (which are passed by reference to the function).

Base case for the recursion is $a = 0$, when the GCD equals b, so the coefficients x and y are 0 and 1, respectively. In all other cases the above formulas are used to re-calculate the coefficients on each iteration.

This implementation of extended Euclidean algorithm produces correct results for negative integers as well.

Practice Problems

- 10104 - Euclid Problem
- GYM - (J) Once Upon A Time
- UVA - 12775 - Gift Dilemma