9th Aug, 2016

Security Lab (CS403)

Laboratory Assignment

Consider the following algorithms for your reference and write the program as per the instructions that follow:

Algorithm Euclidean algorithm for computing the greatest common divisor of two integers

---

INPUT: two non-negative integers a and b with $a \geq b$.
OUTPUT: the greatest common divisor of a and b.

1. While $b \neq 0$ do the following:
   1.1 Set $r \leftarrow a \bmod b$, $a \leftarrow b$, $b \leftarrow r$.
2. Return(a).

Fact Algorithm 2.104 has a running time of $O((\lg n)^2)$ bit operations.

Example (*Euclidean algorithm*) The following are the division steps of Algorithm 2.104 for computing $\gcd(4864, 3458) = 38$:

$$\begin{aligned} 4864 &= 1 \cdot 3458 + 1406 \\ 3458 &= 2 \cdot 1406 + 646 \\ 1406 &= 2 \cdot 646 + 114 \\ 646 &= 5 \cdot 114 + 76 \\ 114 &= 1 \cdot 76 + 38 \\ 76 &= 2 \cdot 38 + 0. \end{aligned}$$

□

Algorithm Extended Euclidean algorithm

INPUT: two non-negative integers a and b with $a \geq b$.
OUTPUT: $d = \gcd(a, b)$ and integers x, y satisfying $ax + by = d$.

1. If $b = 0$ then set $d \leftarrow a$, $x \leftarrow 1$, $y \leftarrow 0$, and return(d,x,y).
2. Set $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$.
3. While $b > 0$ do the following:
   3.1 $q \leftarrow \lfloor a/b \rfloor$, $r \leftarrow a - qb$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$.
   3.2 $a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, and $y_1 \leftarrow y$.
4. Set $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$, and return(d,x,y).

Example (*extended Euclidean algorithm*) Table 2.2 shows the steps of Algorithm 2.107 with inputs $a = 4864$ and $b = 3458$. Hence $\gcd(4864, 3458) = 38$ and $(4864)(32) + (3458)(-45) = 38$. □

q	r	x	y	a	b	x_2	x_1	y_2	y_1
–	–	–	–	4864	3458	1	0	0	1
1	1406	1	−1	3458	1406	0	1	1	−1
2	646	−2	3	1406	646	1	−2	−1	3
2	114	5	−7	646	114	−2	5	3	−7
5	76	−27	38	114	76	5	−27	−7	38
1	38	32	−45	76	38	−27	32	38	−45
2	0	−91	128	38	0	32	−91	−45	128

The table above shows the execution of Extended Euclidean Algorithm with inputs *a=4864, b=3458*

Problem-1: Write a program to solve Linear Diophantine Equation.