The Extended Euclidean Algorithm

BY

V.A.VISHAL RAM

21PC38

INTRODUCTION

- Let a and b be integers, and let d = gcd(a,b).
- We know by Theorem 1.8 that there exist integers s and t such that as + bt = d. The extended Euclidean algorithm allows us to efficiently compute s and t.
- The following theorem defines the quantities computed by this algorithm, and states a number of important facts about them—these will play a crucial role, both in the analysis of the running time of the algorithm, as well as in applications of the algorithm that we will discuss later.

Theorem 1.8. *Let $a, b, r \in \mathbb{Z}$ and let $d := \gcd(a, b)$. Then there exist $s, t \in \mathbb{Z}$ such that $as + bt = r$ if and only if $d \mid r$. In particular, a and b are relatively prime if and only if there exist integers s and t such that $as + bt = 1$.*

Proof. We have

$$\begin{aligned} & as + bt = r \ \text{ for some } s, t \in \mathbb{Z} \\ \iff & r \in a\mathbb{Z} + b\mathbb{Z} \\ \iff & r \in d\mathbb{Z} \ \text{ (by Theorem 1.7)} \\ \iff & d \mid r. \end{aligned}$$

That proves the first statement. The second statement follows from the first, setting $r := 1$. □

Note that as we have defined it, $\gcd(0, 0) = 0$. Also note that when at least one of a or b are non-zero, $\gcd(a, b)$ may be characterized as the *largest* positive integer that divides both a and b, and as the *smallest* positive integer that can be expressed as $as + bt$ for integers s and t.

EXTENDED EUCLIDEAN THEOREM

- **Let $a, b, r_0, \ldots\ldots r_{l+1}$ and $q_1, \ldots.., q_l$ be as in Theorem 4.1.Define integers $s_0, \ldots., s_{l+1}$ and $t_0, \ldots. t_{l+1}$ as follows:**

(i) for $i=0,\ldots,l+1$,we have $as_i + bt_i = r_i$; in particular,$as_l + bt_l = \gcd(a,b)$;

(ii) for $i=0,\ldots,l$, we have $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$;

(iii) for $i=0,\ldots.,l+1$, we have $\gcd(s_i, t_i) = 1$;

(iv) for $i=0,\ldots..,l$, we have $t_i t_{i+1} \leq 0$and $|t_i| \leq |t_{i+1}|$; for $i =1,..,l$, we have $s_i s_{i+1} \leq 0$ and $|s_i| \leq |s_{i+1}|$;

(v) for $i=1,\ldots.,l+1$, we have $r_{i-1}|t_i| \leq a$ and $r_{i-1}|s_i| \leq b$;

(vi) if $a>0$,then for $i=1,\ldots.,l+1$, we have $|t_i| \leq a$ and $|s_i| \leq b$;if $a>1$ and $b>0$, then $|t_l| \leq a/2$ and $|s_l| \leq b/2$

$$
\begin{aligned}
r_0 &= a & r_1 &= b \\
s_0 &= 1 & s_1 &= 0 \\
t_0 &= 0 & t_1 &= 1 \\
&\vdots & &\vdots \\
r_{i+1} &= r_{i-1} - q_i r_i & &\text{and } 0 \le r_{i+1} < |r_i| \qquad \text{(this defines } q_i\text{)} \\
s_{i+1} &= s_{i-1} - q_i s_i \\
t_{i+1} &= t_{i-1} - q_i t_i \\
&\vdots
\end{aligned}
$$

Theorem 4.1. *Let a, b be integers, with $a \geq b \geq 0$. Using the division with remainder property, define the integers $r_0, r_1, \ldots, r_{\ell+1}$, and $q_1, \ldots, q_\ell$, where $\ell \geq 0$, as follows:*

$$
\begin{aligned}
a &= r_0, & & \\
b &= r_1, & & \\
r_0 &= r_1 q_1 + r_2 & & (0 < r_2 < r_1), \\
&\vdots & & \\
r_{i-1} &= r_i q_i + r_{i+1} & & (0 < r_{i+1} < r_i), \\
&\vdots & & \\
r_{\ell-2} &= r_{\ell-1} q_{\ell-1} + r_\ell & & (0 < r_\ell < r_{\ell-1}), \\
r_{\ell-1} &= r_\ell q_\ell & & (r_{\ell+1} = 0).
\end{aligned}
$$

Note that by definition, $\ell = 0$ if $b = 0$, and $\ell > 0$, otherwise.

Then we have $r_\ell = \gcd(a, b)$. Moreover, if $b > 0$, then $\ell \leq \log b / \log \phi + 1$, where $\phi := (1 + \sqrt{5})/2 \approx 1.62$.

4.3 The Principle of Mathematical Induction

Suppose there is a given statement P(n) involving the natural number n such that

(i) *The statement is true for* $n = 1$, i.e., *P*(1) *is true, and*

(ii) *If the statement is true for* $n = k$ *(where* k *is some positive integer), then the statement is also true for* $n = k + 1$, i.e., *truth of P*(k) *implies the truth of P* ($k + 1$).

the **induction step**, proves that *if* the statement holds for any given case $n = k$, *then* it must also hold for the next case $n = k + 1$.

(i) for $i=0,\ldots,l+1$, we have $as_i + bt_i = r_i$; in particular, $as_l + bt_l = \gcd(a,b)$;

Proof: It is easily proved by induction on i. For i = 0,1 , the statement is clear. For i = 2,…..,l+1, we have

$$as_i + bt_i = a(s_{i-2} - s_{i-1}q_{i-1}) + b(t_{i-2} - t_{i-1}q_{i-1})$$

$$= (as_{i-2} + bt_{i-2}) - (as_{i-1} + bt_{i-1})q_{i-1}$$

$$= r_{i-2} - r_{i-1}q_{i-1} \quad \text{(by induction)} \; [as_{i-2} + bt_{i-2} = r_{i-2},\ as_{i-1} + bt_{i-1} = r_{i-1}]$$

$$= r_i.$$

(ii)for i=0,…,l, we have $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$;

Proof: It is also easily proved by induction on i. For i = 0, the statement is clear.
For i = 1,…..,l, we have

$$s_i t_{i+1} – t_i s_{i+1} = s_i(t_{i-1} – t_i q_i) - t_i(s_{i-1} – s_i q_i)$$

$$= -(s_{i-1}t_i – t_{i-1}s_i) \text{ (after expanding and simplifying)}$$

$$= -(-1)^{i-1} \text{ (by induction) } [s_{i-1}t_i – t_{i-1}s_i = (-1)^{i-1}]$$

$$= (-1)^i.$$

(iii)for i=0,….,l+1, we have gcd($s_{i,}t_i$) = 1;

Proof**:** From (ii), $s_{i-1}t_i - t_{i-1}s_i = (-1)^{i-1}$ ➔ Equation(1)

Here s_i and t_i share no common divisors other than 1 and -1.So,s_i and t_i are said to be relatively prime.

From Theorem 1.8, if a and b are relatively prime if and only if there integers s and t such that

$$as + bt = 1 = \gcd(a,b)$$

From Eq(1), $\gcd(s_i,t_i) = 1$

Theorem 1.8. *Let $a, b, r \in \mathbb{Z}$ and let $d := \gcd(a, b)$. Then there exist $s, t \in \mathbb{Z}$ such that $as + bt = r$ if and only if $d \mid r$. In particular, a and b are relatively prime if and only if there exist integers s and t such that $as + bt = 1$.*

Proof. We have

$$\begin{aligned} & as + bt = r \text{ for some } s, t \in \mathbb{Z} \\ \iff & r \in a\mathbb{Z} + b\mathbb{Z} \\ \iff & r \in d\mathbb{Z} \text{ (by Theorem 1.7)} \\ \iff & d \mid r. \end{aligned}$$

That proves the first statement. The second statement follows from the first, setting $r := 1$. □

Note that as we have defined it, $\gcd(0, 0) = 0$. Also note that when at least one of a or b are non-zero, $\gcd(a, b)$ may be characterized as the *largest* positive integer that divides both a and b, and as the *smallest* positive integer that can be expressed as $as + bt$ for integers s and t.

(iv)for i=0,…..,l, we have $t_i t_{i+1} \leq 0$and $|t_i| \leq |t_{i+1}|$; for i =1,..,l, we have $s_i s_{i+1} \leq 0$ and $|s_i| \leq |s_{i+1}|$;

Proof:one can easily prove both statements by induction on i.

The statement involving the t_i's is clearly true for i =0;for i = 1,…..,l, we have $t_{i+1} = t_{i-1} - t_i q_i$, and since by the induction hypothesis t_{i-1} and ti have opposite signs and $|t_i| \geq |t_{i-1}|$, it follows that $|t_{i+1}| = |t_{i-1}| + |t_i| q_i \geq |t_i|$, and that the sign of t_{i+1} is the opposite of that of t_i.

The proof of the statement involving the s_i's is the same, except that we start the induction at i = 1.

(v)for $i=1,\ldots,l+1$, we have $r_{i-1}|t_i| \leq a$ and $r_{i-1}|s_i| \leq b$;

Proof:one considers the two equations:

$$as_{i-1} + bt_{i-1} = r_{i-1}$$
$$as_i + bt_i = r_i$$

Subtracting t_{i-1} times the second equation from t_i times the first, and applying (ii), we get $\pm a = t_i r_{i-1} - t_{i-1} r_i$; consequently, using the fact that t_i and t_{i-1} have opposite sign, we obtain

$$a = |t_i r_{i-1} - t_{i-1} r_i| = |t_i| r_{i-1} + |t_{i-1}| r_i \geq |t_i| r_{i-1}.$$

The inequality involving s_i follows similarly, subtracting s_{i-1} times the second equation from s_i times the first.

(vi) if a>0,then for i=1,….,l+1, we have $|t_i| \le a$ and $|s_i| \le b$;if a>1 and b>0, then $|t_l| \le a/2$ and $|s_l| \le b/2$.

Proof:From (v), if $a > 0$, then $r_{i-1} > 0 \Rightarrow r_{i-1} \ge 1$

$$r_{i-1}|t_i| \le a \Rightarrow |t_i| \le a$$

Similarly for $|si| \le b$ can be proved.

if $a > 1$ and $b > 0$, then $l > 0$ and $r_{l-1} \ge 2$

$$r_{l-1}|t_l| \le a \Rightarrow 2|t_l| \le a$$

$$|t_l| \le a/2$$

Similarly for $|si| \le b/2$ can be proved.

Problems:

1) Suppose a = 100 and b = 35. Then GCD and Find s_i and t_i values,tabulate it with i,r_i and q_i.

i	0	1	2	3	4
r_i	100	35	30	5	0
q_i		2	1	6	

Solution:

Step 1: Using Euclideam algorithm

(1) 100 = 2.35 + 30

(2) 35 = 1.30 + 5

(3) 30 = 6.5 + 0

Therefore GCD(100,35) = 5;

Step 2:Using Method of Back Substitution

5 = 35 – 30 → (2)
= 35 – (100 – 2.35) → (1)[30 = 100 – 2.35]
= – 100 + 3.35 → s_3= -1 and t_3 = 3

Conclusion: So we have gcd(a,b) = 5 = -a + 3b

100 = 1.100 – 0.35(s_0 =1,t_0=0)
35 = 0.100 – 1.35(s_1=0,t_1=1)
30 = 100 – 2.35(s_2=1,t_2=-2)

i	0	1	2	3
r_i	100	35	30	5
q_i		2	1	6
s_i	1	0	1	-1
t_i	0	1	-2	3

2)Suppose a=65 and b=40.let as+bt = gcd(65,40) Find s and t.

Solution:

Step 1:Using Euclidean Algorithm

(1) $65 = 1.40 + 25$

(2) $40 = 1.25 + 15$

(3) $25 = 1.15 + 10$

(4) $15 = 1.10 + 5$

(5) $10 = 2.5$

Therefore: gcd(65,40) = 5

Step 2:Using Method of Back-Substitution

$5 = 15 – 10 \rightarrow (4)$

$= 15 – (25 – 15) \rightarrow (3) = 2.15 - 25$

$= 2(40 – 25) – 25 \rightarrow (2) = 2.40 – 3.25$

$= 2.40 – 3(65-40) = 5.40 – 3.65$

Conclusion:$65(-3) + 40(5) = 5 \rightarrow s=-3,t=5$