Extended Euclid's Algorithm

Udaya Parampalli

Department of Computing and Information Systems
University of Melbourne

July, 2017

Contents

- Basic of Computations on Numbers
- Extended Euclid's Algorithm.

Extended Euclid's algorithm

Let us look at the gcd computation again with general numbers a and b with $a > b > 0$. Let $a_0 = a$, $a_1 = b$ and $q_1 = \lfloor a_0/a_1 \rfloor$.

$$
\begin{array}{cccccc}
 & & & gcd(a_0, a_1) & & \\
a_0 & = & q_1 \times a_1 + a_2 & gcd(a_1, a_2) & q_1 = \lfloor a_0/a_1 \rfloor \\
a_1 & = & q_2 \times a_2 + a_3 & gcd(a_2, a_3) & q_2 = \lfloor a_1/a_2 \rfloor \\
a_2 & = & q_3 \times a_3 + a_4 & gcd(a_3, a_4) & q_3 = \lfloor a_2/a_3 \rfloor \\
 & \vdots & & & \\
a_{t-2} & = & q_{t-1} \times a_{t-1} + a_t & gcd(a_{t-1}, a_t) & q_{t-1} = \lfloor a_{t-2}/a_{t-1} \rfloor \\
a_{t-1} & = & q_t \times a_t + 0 & gcd(a_t, 0) & q_t = \lfloor a_{t-1}/a_t \rfloor
\end{array}
$$

Table: Computation of $gcd(a, b)$

By using the fact on *gcd* before, we have

$$gcd(a, b) = gcd(a_0, a_1) = gcd(a_1, a_2) = \cdots = gcd(a_{t-1}, a_t) = gcd(a_t, 0)$$

Solving for a_t in the above equations starting from last-but-one to the first, we can express a_t as a linear combination of a_0 and a_1.

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

The following example illustrates the above point. A theorem proving version of the algorithm is given at the end of this set of slides.

Extended Euclid's algorithm: Example 1

Consider $gcd(33,21)$:

33	$=$	$1 \times 21 + 12$	$gcd(21,12)$	(A)
21	$=$	$1 \times 12 + 9$	$gcd(12,9)$	(B)
12	$=$	$1 \times 9 + 3$	$gcd(9,3)$	(C)
9	$=$	$3 \times 3 + 0$	$gcd(3,0)$	

Table: Determine $gcd(33,21)$

$$
\begin{array}{cc}
3 = 12 - 1 \times 9 & From(C) \\
3 = 12 - 1 \times (21 - 1 \times 12) & From(B) \\
3 = 2 \times 12 - 1 \times 21 & \\
3 = 2 \times (33 - 1 \times 21) 1 \times 21 & From(A) \\
3 = 2 \times 33 + (-3) \times 21 & Simplification
\end{array}
$$

Computing inverse mod n

If $gcd(n, a)$ is 1 then we can use extended Euclid's algorithm on a and n and get two integers x and y such that

$$xn + ya = 1.$$

Taking mod n on both sides of the above equation we get

$$ya = 1 \bmod n.$$

Clearly y is the inverse of a mod n. Note that the inverse is unique. Also it is clear that if $gcd(n, a) > 1$, then inverse does not exist.

Extended Euclid's algorithm: Example 2

Consider $gcd(13, 25)$:

$$\begin{array}{rcccc} 25 & = & 1 \times 13 + 12 & gcd(13, 12) & (A) \\ 13 & = & 1 \times 12 + 1 & gcd(12, 1) & (B) \\ 12 & = & 12 \times 1 + 0 & gcd(1, 0) & \end{array}$$

Table: Determine $gcd(13, 25)$

$$\begin{array}{cc} 1 = 13 - 1 \times 12 & From(B) \\ 1 = 13 - 1 \times (25 - 1 \times 13) & From(A) \\ 1 = 2 \times 13 - 1 \times 25 & \\ 1 = 2 \times 13 + (-1) \times 25 & Simplification \end{array}$$

It is easy to see now, 2 is inverse of 13 mod 25.

Extended Euclid's algorithm: Theorem Proving version

Theorem

Given two positive integers a and b with $a > b$, let $a_0 = a$, $a_1 = b$ and $q_1 = \lfloor a_0/a_1 \rfloor$. Perform the following matrix equations for $r = 1, 2, \cdots, n$:
$q_r = \lfloor \frac{a_{r-1}}{a_r} \rfloor$,

$$\begin{bmatrix} a_r \\ a_{r+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_r \end{bmatrix} \begin{bmatrix} a_{r-1} \\ a_r \end{bmatrix}$$

until $a_{n+1} = 0$, where n is an integer. Then a_n is the GCD of a and b.

Proof: You can convince that the termination of the algorithm is well defined since $a_{r+1} < a_r$. So eventually, for some n, $a_{n+1} = 0$.

- hence we can write the recursion as the following matrix equation:

$$\begin{bmatrix} a_n \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_n \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{bmatrix} \cdots \begin{bmatrix} 0 & 1 \\ 1 & -q_1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}.$$

Hence, we have

$$\begin{bmatrix} a_n \\ a_{n+1} = 0 \end{bmatrix} = \left\{ \prod_{l=n}^{1} \begin{bmatrix} 0 & 1 \\ 1 & -q_l \end{bmatrix} \right\} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix},$$

Where $\prod$, is the symbol for multiplication. Then, consider only the first row of the above matrix equation, you get $a_n = A_{1,1,}\ a_0 + A_{1,2}\ a_1$, where is the A is the matrix in the RHS of the above equation. Thus any divisor of both $a_0 = a$ and $a_1 = b$ divides a_n. Hence, greatest common divisor $gcd(a, b)$ also divides a_n.

- Further observe that,

$$\begin{bmatrix} 0 & 1 \\ 1 & -q_r \end{bmatrix}^{-1} = \begin{bmatrix} q_r & 1 \\ 1 & 0 \end{bmatrix}$$

and hence by inverting the matrix equation recursively, we get

$$\begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \left\{ \prod_{l=1}^{n} \begin{bmatrix} q_l & 1 \\ 1 & 0 \end{bmatrix} \right\} \begin{bmatrix} a_n \\ 0 \end{bmatrix}.$$

So a_n must divide both $a_0 = a$ and $a_1 = b$ and hence divides $gcd(a, b)$.
Thus $a_n = gcd(a, b)$.

Some implications of the theorem. Let

$$A^r = \left\{ \prod_{l=r}^{1} \begin{bmatrix} 0 & 1 \\ 1 & -q_l \end{bmatrix} \right\} = \begin{bmatrix} 0 & 1 \\ 1 & -q_r \end{bmatrix} A^{r-1}.$$

Theorem

For any integers a and b there exist integers X and Y such that $gcd(a, b) = X\ a + Y\ b.$

Proof

From Theorem 1, we have

$$\begin{bmatrix} a_n \\ 0 \end{bmatrix} = A^n \begin{bmatrix} a \\ b \end{bmatrix}.$$

Hence $gcd(a, b) := a_n = A^n_{11}\ a + A^n_{12}\ b.$

Similarly prove the following theorem.

Theorem

The matrix elements A^n_{21} and A^n_{22} satisfy
$a = (-1)^n A^n_{22}\ gcd(a, b)$
$b = (-1)^n A^n_{21}\ gcd(a, b)$.