Week 2

Lecture 1

Extended GCD Algorithm

Udaya Parampalli

School of Computing and Information Systems
University of Melbourne

Lecture 1

Part -1 Extended GCD Algorithm and Related Computations

Part -2 Symmetric key Cryptography

Lecture 2

Properties of Numbers

Workshop 2: Workshops start from this week

Quizz 2

1.1 Extended GCD Algorithm: A direct version

- Algorithm
- An example.

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 $q_1 = \lfloor a_0/a_1 \rfloor$

			$gcd(a_0, a_1)$	
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}	$=$	$q_t \times a_t + 0$	$gcd(a_t, 0)$	$q_t = \lfloor a_{t-1}/a_t \rfloor$

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.

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 $gcd(33, 21)$

$$3 = 12 - 1 \times 9 \qquad From(C)$$
$$3 = 12 - 1 \times (21 - 1 \times 12) \qquad From(B)$$
$$3 = 2 \times 12 - 1 \times 21$$
$$3 = 2 \times (33 - 1 \times 21) - 1 \times 21 \qquad From(A)$$
$$3 = 2 \times 33 + (-3) \times 21 \qquad Simplification$$

1.2 Inverse Mod n

- Definition
- Inverse mod n Computation
- Computation with Magma

Let a and b be integers and let n be a positive integer.
We say "a" is congruent to "b", modulo n and write

$$a \equiv b \ (mod \ \ n),$$

if a and b differ by a multiple of n; i.e ; if n is a factor of $|b - a|$.
Every integer is congruent mod n to exactly one of the integers in the set

$$Z_n = \{0, 1, 2, \cdots, n - 1\}.$$

We can define the following operations:

$$x \oplus_n y = (x + y) \ mod \ n.$$

$$x \otimes_n y = (xy) \ mod \ n$$

When the context is clear we use the above special addition and multiplication symbols interchangeably with their counterpart regular symbols.

Definition

Let $x \in Z_n$, if there is an integer y such that

$$x \otimes_n y = 1,$$

then we say y is the multiplicative inverse of x. It is denoted by $y = x^{-1}$ usually.

Example: let $n = 5$, 2 is inverse of 3 in Z_5. Or in other words 2 is inverse of 3 modulo 5.

Fact

For any integers a and b, there exist integers x and y such that

$$gcd(a, b) = ax + by.$$

You can determine x and y by modifying Euclid's algorithm for $gcd(a, b)$. Thus we can say that we can find inverse of a modulo b provided $gcd(a, b) = 1$.

Computing inverse mod n

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

$$xa + yn = 1.$$

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

$$xa = 1 \bmod n.$$

Clearly x is the inverse of a mod n.

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. **Note**: *The output of the extended gcd algorithm which is the inverse of a given integer depends on the order of the input arguments.*

Extended Euclid's algorithm: Example 2

Consider $gcd(13, 25)$:

25	$=$	$1 \times 13 + 12$	$gcd(13, 12)$	(A)
13	$=$	$1 \times 12 + 1$	$gcd(12, 1)$	(B)
12	$=$	$12 \times 1 + 0$	$gcd(1, 0)$	

Table: Determine $gcd(13, 25)$

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

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

Magma is a symbolic mathematical software package which can help you to do computations in algebra, number theory and geometry.

http://magma.maths.usyd.edu.au/magma/

An online calculator is available here:

http://magma.maths.usyd.edu.au/calc/

==

ExtendedGreatestCommonDivisor(m, n) : RngIntElt, RngIntElt →RngIntElt,
RngIntElt, RngIntElt

Xgcd(m, n) : RngIntElt, RngIntElt → RngIntElt, RngIntElt, RngIntElt

XGCD(m, n) : RngIntElt, RngIntElt → RngIntElt, RngIntElt, RngIntElt

==

The extended GCD of m and n; returns integers g, x and y such that g is the greatest common divisor of the integers m and n, and g = x.m + y.n. If m and n are both zero, g is zero; otherwise g is always positive. If m and n are both non-zero, the multipliers x and y are unique.

1.3 Extended GCD 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 $\prod_l$ 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
$a = (-1)^n A^n_{22}\ gcd(a, b)$
$b = (-1)^n A^n_{21}\ gcd(a, b)$.

Week 2

Lecture 1

Part -1 Extended GCD Algorithm and Related Computations

Part -2 Symmetric key Cryptography

Lecture 2

Properties of Numbers

Workshop 2: Workshops start from this week

Quizz 2