25-09-2008

Recap:

* proved Division Theorem

$$m = nq + r \quad (0 \le r < n)$$

* GCD Algo:

$$\gcd(m, n) = \gcd(n, r)$$

$$\gcd(n, 0) = n$$

* Inverse a' of a in Z_n

$$a' \cdot_n a = 1$$

* Lemma 2.5

a has inverse in Z_n $\Rightarrow$ $a \cdot_n x = b$ has unique solution

Proof of Theorem 2.7

* Let a' be an inverse of a. Z_n

$\Rightarrow$ $a \cdot_n a' = 1$

$\Rightarrow$ It is a solution to

$$a \cdot_n x = 1 \qquad (*)$$

$\Rightarrow$ According Lemma 2.5, $(*)$ has only <u>one possible</u> solution

$\Rightarrow$ a' must be unique

Proved.

More examples on the use of Corollary 2.6

* $3 \cdot_6 X = 2$ $(*)$

$\Rightarrow 3X$: multiple of 3

$\Rightarrow 3X \bmod 6$: multiple of 3

$\Rightarrow$ can never be 2.

$\Rightarrow (*)$ has no solution

$\Rightarrow$ 3 has no inverse in Z_6

* 6 has no inverse in Z_9

$6 \cdot_9 X = 2$ $(**)$

$\Rightarrow 6X$: multiple of 3

$\Rightarrow 6X \bmod 9$: multiple of 3

$\Rightarrow (**)$ has no soln

$\Rightarrow$ 6 has no inverse in Z_9.

Lemma 2.8: $a \cdot_n x = 1$ has soln in $\mathbb{Z}_n$

$\Longleftrightarrow$ $ax + ny = 1$ for some integers x & y

Proof: $\Rightarrow$:

Exist $b \in \mathbb{Z}_n$, $a \cdot_n b = 1$

$\Rightarrow$ $ab \bmod n = 1$

$\Rightarrow$ $ab = qn + 1$

$\Rightarrow$ $ab + n(-q) = 1$

$\Rightarrow$ $ax + ny = 1$: $x = b$, $y = -q$

$\Leftarrow$: Exist x & y, $ax + ny = 1$

$\Rightarrow$ $ax = (-y)n + 1$

$\Rightarrow$ $ax \bmod n = 1$

$\Rightarrow$ $(a\,(x \bmod n)) \bmod n = 1$

$\Rightarrow$ $ab \bmod n = 1$, $b = x \bmod n$

$\Rightarrow$ $a \cdot_n b = 1$, $b \in \mathbb{Z}_n$

proved.

Theorem 2.9: a has inverse in Z_n

$\Longleftrightarrow$ $ax + ny = 1$ for some integers x & y

Corollary of Lemma 2.8

Corollary 2.10: If exist integer x, y, s.t.

$$ax + ny = 1.$$

then inverse of a in Z_n is

$$x \bmod n$$

Follows from 2nd part of the proof of Lemma 2.8.

How do we find x & y?

Link it to gcd.

Lemma 2.11 : $a, n > 0$, integers

$ax + ny = 1$ for some integers x, y

$\Longrightarrow \gcd(a, n) = 1$

---

proof : Suppose $k \mid a$, $k \mid n$, $k > 0$

$\Longrightarrow$ $a = s \cdot k$, $n = qk$ for some s, q

$$1 = ax + ny$$

$$= skx + qky$$

$$= (sx + qy)k \qquad \star$$

$\Longrightarrow k \mid 1$

$\Longrightarrow k = 1$. $\Longrightarrow \gcd(a, n) = 1$

proved.

Extended GCD Algo

* Input: $a, n > 0$, integers
* Output:
  - $\gcd(a, n)$
  - x, y s.t.

$$ax + ny = \gcd(a,n)$$

Questions

1. Does a have inverse in Z_n?

   <u>Answer</u>: yes iff $\gcd(a,n) = 1$

2. How to find inverse of a?

   <u>Answer</u>: $a^{-1} = x \bmod n$

Extended GCD Algo

$\boxed{\text{Slide } 45}$

* Have:

$$k = jq + r \qquad (1)$$

$$x', y': \quad rx' + jy' = gcd(r, j) \qquad (2)$$

* Find x, y s.t.

$$jx + ky = gcd(j, k) \qquad (*)$$

$(1) \Rightarrow \quad r = k - jq \qquad (3)$

$(3) + (2) \Rightarrow \quad (k - jq)x' + jy' = gcd(r, j)$

$\Rightarrow \quad j(y' - qx') + kx' = gcd(j, k)$

So, if we set

$$x = y' - qx', \quad y = x'$$

then $(*)$ is satisfied.

Extended GCD Algo : Example

$K = 24$, $j = 14$

$\boxed{x = y' - q x' , \quad y = x'}$

$K = j \cdot q + r$	x	y	x'	y'
$24 = 14 \cdot 1 + 10$	-5	3	3	-2
$14 = 10 \cdot 1 + 4$	3	-2	-2	1
$10 = 4 \cdot 2 + 2$	-2	1	1	0
$4 = 2 \cdot 2$	1	0		

$gcd = 2$ $\qquad x = -5 , \quad y = 3$

$$jx + ky = gcd(j, k)$$

$$14 \cdot (-5) + 24 \cdot 3 = -70 + 72 = 2$$