30-09-2008 : Recap

* Lemma 2.15 :

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

- Theorem 2.7 : inverse unique
- Corollary 2.6 : way to show no inverse

* Lemma 2.8

$a \cdot_n x = 1$ has soln $\Leftrightarrow$ $ax + ny = 1$ for some x & y

Th 2.9 $\Leftrightarrow$ a has inverse

Cor 2.10 inverse : x mod n

* Lemma 2.11

$ax + ny = 1$ for some x & y $\Rightarrow$ $\gcd(a, n) = 1$

* Extended GCD

Extended GCD Algo: Example

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

GCD(k, j)	$k = j \cdot q + r$	gcd	x	y	x'	y'
GCD(201, 65)	$201 = 65 \cdot 3 + 6$	1	-34	11	11	-1
GCD(65, 6)	$65 = 6 \cdot 10 + 5$	1	11	-1	-1	1
GCD(6, 5)	$6 = 5 \cdot 1 + 1$	1	-1	1	1	0
GCD(5, 1)	$5 = 1 \cdot 5$	1	1	0		

$$jx + ky = 65 \cdot (-34) + 201 \cdot 11$$
$$= -2210 + 2211 = 1 = \gcd(k, j)$$

65 has inverse in Z_{201}. It is $-34 \bmod 201 = 167$

$\boxed{L15-16}$

Corollary of Theorem 2.14

Exist x & y s.t.

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

$\Rightarrow$ If $\gcd(j,k) = 1$, exist x, y s.t.

$$jx + kj = 1 \qquad (*)$$

Lemma 2.11 $(**)$

$$jx + kj = 1 \Rightarrow \gcd(j,k) = 1$$

$(*) + (**) \Rightarrow$

Theorem 2.15:

$\gcd(j,k) = 1 \Leftrightarrow jx + kj = 1$ for some x & y

Running Time of GCD / Extended GCD

* GCD(j, k) $(0 \le j < k)$

  takes at most $2\log_2 k$ steps

  k

$$k^2 \to k\log k$$

Summary of Lecture 5

$\boxed{a \text{ has inverse in } \mathbb{Z}_n}$

$\Updownarrow$ Lemma 2.15

$\boxed{a \cdot_n x = 1 \text{ has soln}}$

$\Updownarrow$ Lemma 2.8. Th 2.9

$\boxed{ax + ny = 1 \text{ for some } x \text{ \& } y}$

$\Updownarrow$ Th 2.15

$\boxed{\gcd(a, n) = 1}$

Extended GCD(k, j)

- $\gcd(k, j)$
- x, y s.t

$$jx + ky = 1$$

Used to find inverse.