Lecture 5

Objectives

* Resolve issues from L4
  * prove Division Theorem
  * Inverse for $f_{a.n}(x) = a \cdot_n x$
* Tools for next lecture
  * Greatest Common Divider (GCD) concept, algo
  * Inverse of a in Z_n

---

* Inverse & equation $a \cdot_n X = b$
* $a \cdot_n X = 1$ & $ax + ny = 1$
* Extended GCD Algo: find x.y s.t. $ax + ny = \gcd(a, n)$
* $X = a^{-1}$ when $\gcd(a.n) = 1$.

Proof by Contradiction

* Need to prove: p is true

* Strategy
  * Assume p is false
  * Derive contradiction.
  * Conclude: p must be true.

First step in proving Theorem 2.12

* Need to prove: For any $m \geq 0$,

  Exist q & r, s.t. $m = qn + r$ $(0 \leq r < n)$

* Proof by contradiction

  * Assume exist $m \geq 0$, s.t.

    $$m = qn + r \qquad (*)$$

    not true for any q, r $(0 \leq r < n)$

  * Choose the <u>smallest</u> such m.

  * If $m < n$,

    $$m = 0 \cdot n + m \qquad (0 \leq m < n)$$

    $(q = 0,\ r = m)$ satisfies $(*)$

    Contradiction!

* If $m \geq n$

- Let $m' = m - n$, $m' \geq 0$
- $m' < m$. There must exist q', r'

s.t. $m' = q'n + r'$ $(0 \leq r' < n)$

$\Rightarrow$ $m - n = q'n + r'$

$\Rightarrow$ $m = (1+q')n + r'$

Contradicts the choice of m!

proof. completed

Proof of Theorem 2.12
2nd step

* Need to prove:

$$m = qn + r \quad (0 \le r < n) \qquad (*)$$

$$m = q'n + r' \quad (0 \le r' < n) \qquad (**)$$

$\Rightarrow q = q', \quad r = r'$

* Substract $(*)$ and $(**)$:

$$0 = (q - q')n + r - r'$$

$$\Rightarrow (q' - q)n = r - r'$$

$$\Rightarrow |q' - q|\, n = |r - r'|$$

$$|r - r'| < n$$

$$\Rightarrow |q' - q|\, n < n \qquad ☆$$

$$\Rightarrow |q' - q| = 0 \quad \Rightarrow q' = q$$

$$\Rightarrow r' = r.$$

proved.

Proof of Lemma 2.13

Proof

$$\boxed{\begin{array}{l} k = jq + r \\ \gcd(k, j) = \gcd(j, r) \end{array}}$$

* Case 1: $r = 0$

$\Rightarrow k = jq$, $j \mid k$

we have: $j \mid j$, $\gcd(j, k) \leq j$

$\Rightarrow \gcd(j, k) = j$

$j \mid j$, $j \mid 0$, $\gcd(j, 0) \leq j$

$\Rightarrow \gcd(j, 0) = j$

$\Rightarrow \gcd(j, k) = \gcd(j, r)$

* case 2: $r > 0$

will show:

$$d \mid j,\ d \mid k \iff d \mid j,\ d \mid r \quad (*)$$

$$\Rightarrow \gcd(j,k) = \gcd(r,j)$$

---

proof of (*)

$\Rightarrow$: $d \mid j,\ d \mid k$

$$\Rightarrow k = i_1 d,\quad j = i_2 d$$

$$\Rightarrow j = i_2 d,\quad r = k - jq$$

$$= i_1 d - i_2 d q$$

$$= (i_1 - i_2 q) d$$

$$\Rightarrow d \mid j,\ d \mid r.$$ proved.

$\Leftarrow$: Similar

Lemma proved.