Mo Day Yr _____ day Event: _____ Venue: (1)

Extended Euclidean Algorithm:

Th: Given $a, b \in \mathbb{Z}$, $b>0$, $\exists$ unique $q, r \in \mathbb{Z}$ s.t.

1) $0 \leq r < b$

2) $a = qb + r$

▷ Choose the integer

$$q = \left\lfloor \frac{a}{b} \right\rfloor$$

then $r = \frac{a}{b} - q < 1$

or $r = 0$ when $b \mid a$.

Hence 1), 2) are satisfied.

Since q is unique r is also unique

By successive division, let

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$\vdots$$

Since $r_1 < b$, $r_2 < r_1$, $r_3 < r_2$ ... there is n s.t. $r_{n+1} = 0$, i.e.

$$r_{n-1} = q_{n+1} r_n$$

Hence $r_n \mid r_{n-1}$. Let for example $n = 2$

then

$$r_1 = q_3 r_2 + 0$$

Hence $r_2 \mid r_1$, $r_2 \mid b$, $r_2 \mid a$.

By induction,

$$r_n \mid a, b$$

If $d \mid a, b$ then $d \mid r_n$.

Hence $r_n = (a, b)$

These eqns can be written as

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} b \\ r_1 \end{bmatrix}$$

$$= \begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} q_2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \end{bmatrix}$$

$$= \begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} q_2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} q_3 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} r_2 \\ 0 \end{bmatrix}$$

(since $r_3 = 0$). Hence

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} r_2 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} r_2 \\ 0 \end{bmatrix} = \begin{bmatrix} x & y \\ * & * \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} \qquad \begin{bmatrix} x & y \\ * & * \end{bmatrix} = \begin{bmatrix} p & q \\ r & s \end{bmatrix}^{-1}$$

This gives expression of gcd (a, b) as an integral linear combination of a, b :

Example: $a = 235 \quad b = 124$

$$\frac{a}{b} = 1.895 \qquad q_1 = 1$$

$$r_1 = 235 - 1 \times 124 = 111$$

$$\frac{124}{111} = 1.117 \qquad q_2 = 1$$

$$r_2 = 124 - 1 \times 111 = 13$$

$$\frac{111}{13} = 8.538 \qquad q_3 = 8$$

$$r_3 = 111 - 8 \times 13 = 7$$

$$\frac{13}{7} = 1.857 \qquad q_4 = 1$$

$$r_4 = 13 - 1 \times 7 = 6$$

~~Hence gcd (235, 124) = 7~~

$$\frac{7}{6} = 1.1666 \qquad q_5 = 1$$

$$r_5 = 7 - 1 \times 6 = 1$$

$$\frac{6}{1} = 6 \qquad q_6 = 6$$

$$r_6 = 6 - 6 \times 1 = 0$$

Hence gcd (235, 124) = 1

$$\begin{bmatrix} p & q \\ r & s \end{bmatrix}^{-1} = \begin{bmatrix} 6 & 1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 8 & 1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{-1}$$

$$= \begin{bmatrix} 0 & 1 \\ 1 & -6 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -8 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & -1 \\ -6 & 7 \end{bmatrix} \begin{bmatrix} 1 & -8 \\ -1 & 9 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & -17 \\ -13 & \underline{48+63} \\ & 111 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 19 & -36 \\ * & * \end{bmatrix}$$

$19 \times 235 - 36 \times 124 = 1$

Mo. Day Yr. day Event: Venue:

(5)

Residue class ring $\mathbb{Z}_n$

(Numbers modulo n)

$\mathbb{Z}_n = \{[0], [1], [2], \cdots [n-1]\}$

$[r] \boxplus [s] = [r+s \bmod n]$

$[r] \odot [s] = [rs \bmod n]$

If $[r] \odot [s] = [1]$ then $[s]$ is inverse of $[r]$ in $\mathbb{Z}_n$.

$[r] \odot [s] = 1 \Leftrightarrow \{rs = 1 \bmod n\}$

$\Leftrightarrow rs - 1 = 0 \bmod n$

$\Leftrightarrow n \mid (rs-1)$

$\Leftrightarrow \exists\, q$ s.t.

$rs + qn = 1.$

By extended Euclid,

if $d = (a, b)$ $\exists$ x, y s.t.

$d = ax + by.$ $(d) = I(a, b)$

Hence if $\tilde{d} = a\tilde{x} + b\tilde{y}$

then $d \mid \tilde{d}$.

Hence $(r, n) = 1$, $s = x \bmod n$

Example: Find $\bar{3}^{-1}$ mod 17

Since $1 = 3 \times 6 - 1 \times 17$

$[3] \odot [6] = [1]$

Since $3 \times 6 = 1 \bmod 17$.

Hence $[3]^{-1} = [6]$

Order of an element:

If $a \in \mathbb{Z}_n$ and d is smallest non-neg. number s.t.

$a^d = 1$ in $\mathbb{Z}_n$

d is called order of a.

Examples:

1) Find ord(3) in $\mathbb{Z}_{17}$

powers $3,\ 3^2 = 9,\ 3^3 = 10,\ 3^4 = 13,$

$3^5 = 5,\ 3^6 = 15,\ 3^7 = 11,\ 3^8 = 16$

$3^9 = 14,\ 3^{10} = 8,\ 3^{11} = 7,\ 3^{12} = 4,$

$3^{13} = 12,\ 3^{14} = 2,\ 3^{15} = 6,\ 3^{16} = 1$

Hence order $3 = 16$ in $\mathbb{Z}_{17}$

1) If $n=p$ is prime then every non-zero element in $\mathbb{Z}_p$ has an inverse. Hence $\mathbb{Z}_p$ is a field of p elements

$$\mathbb{Z}_p = \{0, 1, 2, \cdots p-1\}$$

The set $\mathbb{Z}_p^* = \{1, 2, \cdots p-1\}$ is a group since every element has inverse.

2) For $p=17$ consider $a=2$ in $\mathbb{Z}_p^*$

powers of 2 are

$$2,\ 2^2=4,\ 2^3=8,\ 2^4=16,$$
$$2^5=15,\ 2^6=13,\ 2^7=9,\ 2^8=1$$

Hence order $2 = 8$

// Order of an element $|\ p-1$ // (*)

By Lagrang's Theorem because $p-1 = |\mathbb{Z}_p^*|$ the cardinality of the group $\mathbb{Z}_p^*$ also called order of $\mathbb{Z}_p^*$

// Try to give your own proof of (*) //

3) Fermat's Little Theorem:

If p is prime and $p \nmid a$ then

$$\boxed{a^{p-1} = 1 \bmod p}$$

This is same as the statement that $\text{order}(a \bmod p) \mid p-1$

Hence $(a \bmod p)^{p-1} = 1$ in $\mathbb{Z}_p^*$

4) In general if G is a group, $a \in G$ then $\text{ord}\, a \mid \text{ord}\, G = |G|$

An element $g \in G$ is called primitive if $\text{ord}\, g = |G|$.

Example: 3 is primitive in $\mathbb{Z}_{17}^*$

2 is not primitive in $\mathbb{Z}_{17}^*$

Find ord 2 in $\mathbb{Z}_{13}^*$ is 2 primitive?

Example: Compute

$$7^{1001} \bmod 101$$

$$= 7^{(1001 \bmod 100)} \bmod 101$$

$$= 7$$

(since by Fermat's theorem: $a^{p-1} = 1 \bmod p$ and 101 is prime).