Note Title 12/1/2010

① $\langle 12 \rangle$ in U_{19}

$12^2 \equiv 11$

$12^3 \equiv 18$

$12^4 \equiv 7$

$12^5 \equiv 8$

$12^6 \equiv 1$

$\langle 12 \rangle = \{12, 11, 18, 7, 8, 1\}$

$|U_{19}| = |\langle 12 \rangle| \cdot \text{index}$

$\underbrace{|U_{19}|}_{18} = \underbrace{|\langle 12 \rangle|}_{6} \cdot \underbrace{\text{index}}_{3}$

$2\langle 12 \rangle = \{5, 3, 17, 14, 16, 2\}$

$4\langle 12 \rangle = \{10, 6, 15, 9, 13, 4\}$

$U_{19} = \langle 12 \rangle \cup 2\langle 12 \rangle \cup 4\langle 12 \rangle$

(disjoint) (disjoint)

② Suppose $xH = yH$.

Then $\exists h, h' \in H$ $\quad xh = yh'$

$xy^{-1} = h'h^{-1} \in H$

Conversely suppose $xy^{-1} \in H$, then $\exists h \in H$

$xy^{-1} = h$, $x = yh$, $x \in yH$, $xH \subseteq yH$

$y = xh^{-1} \in xH$, $yH \subseteq xH$

$\therefore xH = yH$ ☺

(3) Suppose $\langle x \rangle = \mathbb{Z}_m$

$= \{jx : j \in \mathbb{Z}\}$

Since $1 \in \mathbb{Z}_m$, $1 \in \langle x \rangle$.

Suppose $1 \in \langle x \rangle$. then $1 = jx$ for some $j \in \mathbb{Z}$

Let $[y]_m \in \mathbb{Z}_m$, then $y = (yj)x \quad \therefore y \in \langle x \rangle$

Suppose $1 \in \langle x \rangle$, then $1 \equiv jx \pmod m$ for some $j \in \mathbb{Z}$

$1 = jx + km$ for some k

$\uparrow$ $\therefore \gcd(x, m) = 1$

Conversely if $\gcd(x,m) = 1$, By Bezout

$\exists\, s, t \in \mathbb{Z} \qquad 1 = sx + tm$

$\therefore 1 \equiv sx \pmod m$

$\therefore 1 \in \langle x \rangle$ ☺

④ $\gcd(9, 30) = 3$

$3 \nmid 28$

$\therefore$ no solutions.

⑤ $u_7 = [1, 2, 3, 4, 5, 6]$

$2u_7 = [2, 4, 6, 1, 3, 5]$

$3u_7 = [3, 6, 2, 5, 1, 4]$

$4u_7 = [4, 1, 5, 2, 6, 3]$

$5u_7 = [5, 3, 1, 6, 4, 2]$

$6u_7 = [6, 5, 4, 3, 2, 1]$

Define f by a table:

x	$f(x)$
1	$()$
2	$(124)(365)$
3	(132645)
4	$(142)(356)$
5	(154623)
6	$(16)(25)(34)$