1. (a)

$U_n := \{m \mid 0 \le m \le n-1, (m,n)=1\}$

$U_{100} = 100(1-\frac{1}{2})(1-\frac{1}{5}) = 40$

(b)

"closed"

Let $k, m \in U_n \Rightarrow 0 \le k, m \le n-1$

$(k,n)=1, (m,n)=1$.

Assume $km = an + r \equiv r \pmod{n}$

Claim: $(r,n)=1$

Suppose $(r,n) = d > 1, d = p^h$, $p : prime$

$\because d \mid n$, $d \mid r$ and $p \mid d$

$\therefore p \mid n$, $p \mid r$

$\therefore p \mid km \Rightarrow p \mid k$ or $p \mid m$

$\therefore (k,n) \neq 1$ or $(m,n) \neq 1$ $\rightarrow\leftarrow$

$\therefore (r,n)=1$

"identity"

$1 \in U_n$, $1 \cdot m = m = m \cdot 1$, $\forall m \in U_n$

"associative"

Let $m, k, p \in U_n$

$\Rightarrow (mk)p \equiv mkp \equiv m(kp) \pmod{n}$

"inverse"

Let $m \in U_n$, $(m,n)=1$

$\Rightarrow am + bn = 1$

$\Rightarrow am \equiv 1 \pmod{n}$

$\therefore (a,n)=1$

Assume $a = kn + r'$, $0 \le r' \le n-1$, $k \in \mathbb{Z}$

$\therefore am \equiv r'm \pmod{n} \equiv 1$

$\therefore r' = m^{-1} \in U_n$

(c)

$U_p = \{1, 2, \ldots, p-1\}$, $|U_p| = p-1$.

$(U_p, \bullet)$ is a group by (b).

(1) If a=0, $a^p = 0^p = 0 = a \pmod{n}$

(2) If $0 < a \le p-1$, let $|a| = k$.

$a^k \equiv 1 \pmod{p}$

By Lagrange Theorem $k \mid p-1$

$\Rightarrow a^{p-1} = a^{km}$ for some $m \in \mathbb{Z}$

$= (a^k)^m = 1^m \equiv 1 \pmod{p}$

$\Rightarrow a^p \equiv a \pmod{p}$

(3) If $a \ge p$, let $a = n \cdot p + r$ for some $n \in \mathbb{Z}$ and $0 \le r \le p-1$

$a^p = (np+r)^p \equiv r^p \pmod{p}$

$\equiv r \pmod{p}$

$\equiv a \pmod{p}$

(d)

Suppose $< a >= U_p$

By (c) we know that $a^{p-1} \equiv 1 \pmod{p}$

Since $q \mid p-1$, $\exists l \in \mathbb{N}$ *s.t* $ql = p-1$

Claim: $a^l$ is the s we want.

$(a^l)^q = a^{lq} = a^{p-1} \equiv 1 \pmod{p}$

Hence we find such $s = a^l \neq 1$