DEFINITION (Reduced set mod m).

A sequence of $\varphi(m)$ integers $a_1, \dots, a_{\varphi(m)}$ is called a reduced set mod m if

(i) $i \neq j \Rightarrow a_i \not\equiv a_j \pmod{m}$;

(ii) $\gcd(a_i, m) = 1$ for $1 \leq i \leq \varphi(m)$.

THEOREM If $a_1, \dots, a_{\varphi(m)}$ form a reduced set mod m & $\gcd(b, m) = 1$, then

$$ba_1, \dots, ba_{\varphi(m)}$$

also form a reduced set mod m.

THEOREM (Solving a linear congruence)

The congruence $ax \equiv b \pmod{m}$ (1)

is soluble if and only if $d = \gcd(a, m)$ divides b. The solution is unique mod $\frac{m}{d}$ ie consists of a congruence class mod m/d or d solutions mod m.

PROOF (i) Suppose $ax \equiv b \pmod{m}$ holds. Then $ax = b + km$.

Now $d | a$ & $d | m$. Hence $d | b$.

(ii) Suppose $d | b$. Then (1) is equivalent to

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\text{mod}\, \frac{m}{d}\right). \qquad (2)$$

But $\gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1$.