Linear Equations in $\mathbb{Z}_n$

Consider the equation

$$ax = b$$

where $a, b \in \mathbb{Z}_n$, $a \neq 0$ and the operations are those of $\mathbb{Z}_n$. We can also write such an equation in the form

$$ax \equiv b \pmod{n}$$

where x is to come from $[n]$

Observation If $\gcd(a, n) = 1$ then the equation has the unique solution
$$x = a^{-1} b$$
for each possible $b \in \mathbb{Z}_n$

What if $\gcd(a, n) = d > 1$? ?

Discussion Suppose $\exists\ x \in \mathbb{Z}$ s.t

$$ax = b \pmod{n}$$

Then $\quad n \mid ax - b$

Set $\quad a = a'd$ and $n = n'd$ so that

$$n'd \mid a'xd - b$$

But then d MUST divide b

<u>Conclusion</u> If $ax \equiv b \pmod{n}$ has a solution then $\gcd(a,n) \mid b$.

<u>More Discussion</u> Suppose $d = \gcd(a,n)$ does divide b and set

$$n = n'd \;,\; a = a'd \text{ and } b = b'd.$$

<u>Claim</u> $x \in \mathbb{Z}$ is a solution of

$$ax \equiv b \pmod{n}$$

iff

$$a'x \equiv b' \pmod{n'}$$

Pf/ $\quad n \mid ax - b \iff n' \mid a'x - b'$

<u>Claim</u> $a'x \equiv b' \pmod{n'}$ has a UNIQUE solution in $\mathbb{Z}_{n'}$, say x_1

Pf/ $\gcd(a', n') = 1 \implies (a')^{-1}$ exists in $\mathbb{Z}_{n'}$ and so

$$a'x = b' \quad \text{in } \mathbb{Z}_{n'}$$

iff

$$x = (a')^{-1} b \quad \text{in } \mathbb{Z}_{n'}$$

<u>Observation</u> Every other solution of

$$a'x \equiv b' \pmod{n'}$$

must be congruent to $x_1 \pmod{n'}$

Pf/ If $a'x_2 \equiv b' \pmod{n'}$ then

$$a'(x_2 - x_1) \equiv 0 \pmod{n'}$$

i.e $\quad n' \mid a'(x_2 - x_1)$

But $\gcd(n', a') = 1 \implies n' \mid x_2 - x_1$

<u>Conclusion</u> The other solutions of $a'x \equiv b' \pmod{n'}$ (and therefore also of $ax \equiv b \pmod{n}$) in $\mathbb{Z}_n$ are

$$x_1 + n',\ x_1 + 2n',\ \ldots,\ x_1 + (d-1)n'$$

Ex $\quad 8x \equiv b \pmod{12}$

Realize $\gcd(8,12) = 4$ so the b's in $\mathbb{Z}_{12}$ for which there are solutions are

$$0, 4, 8$$

$b = 0$: $\quad 8x \equiv 0 \quad x = 0, 3, 6, 9$

$b = 4$: $\quad 8x \equiv 4 \quad x = 2, 5, 8, 11$

$b = 8$: $\quad 8x \equiv 8 \quad x = 1, 4, 7, 10$