Solve the following equations in $\mathbb{Z}_{14}$. Express answers as $[x]$ where $0 \leq x < 14$.

ii) $[10][x] = [1]$

iii) $[10][x] = [2]$

$\Leftrightarrow 10x \equiv 1 \bmod 14$

$\because \gcd(10, 14) = 2 \nmid 1$

by LCT 1, this has no solutions

(iii) $[10][x] = [2] \Leftrightarrow 10x \equiv 2 \bmod 14$

Since $10(3) \equiv 30 \equiv 2 \bmod 14$

LCT 1 says $x \equiv 3 \bmod \frac{14}{\gcd(10,14)}$

is the complete solution.

ie $x \equiv 3 \bmod 7$

ie $X \equiv 3, 10 \bmod 14$

ie $[x] = [3]$ or $[10]$ in $\mathbb{Z}_{14}$.

Solve the following equations in $\mathbb{Z}_{14}$. Express answers as $[x]$ where $0 \leq x < 14$.

ii) $[10][x] = [1]$ $\Leftrightarrow$ $10x \equiv 1 \mod 14$

iii) $[10][x] = [2]$

$\therefore \gcd(10,14) = 2 \nmid 1$

by LCT 1, this has no solutions.

(iii) $[10][x] = [2] \Leftrightarrow 10x \equiv 2 \mod 14$

$\Leftrightarrow$ Solve the LDE

$10x + 14y = 2$

$5x + 7y = 1$

By LDET2 $x = 3 + 7n$ $\forall n \in \mathbb{Z}$

$y = -2 - 5n$

$\therefore x \equiv 3 \mod 7$

$\therefore x \equiv 3, 10 \mod 14$

$\therefore [3]$ & $[10]$ are our solutions.

Inverses

- $[-a]$ is the additive inverse of $[a]$, that is,
$$[a]+[-a]=[0].$$
- If $\exists\, b \in \mathbb{Z}$ s.t. $[a][b]=[1]=[b][a]$
we call $[b]$ the multiplicative inverse of $[a]$ and write $[b]=[a]^{-1}$

Ex: $[5][11]=[1]$ in $\mathbb{Z}_{18}$
$\therefore [5]^{-1}=[11]$ & $[11]^{-1}=[5]$

WARNING: Multiplicative inverses do <u>not</u> always exist!

Ex: $[9][x]=[1]$ in $\mathbb{Z}_{18}$
LHS is <u>always</u> $[0]$ or $[9]$.
So $[9]^{-1}$ does not exist in $\mathbb{Z}_{18}$.

Find the additive and multiplicative inverses of $[7]$ in $\mathbb{Z}_{11}$. Give your answers in the form $[x]$ where $0 \leq x \leq 10$.

Soln: Additive Inverse

$[-7] = [4]$.

Multiplicative Inverse: Want to Solve

$[7][x] = [1]$

$\iff 7x \equiv 1 \mod 11$

$7 \cdot 3 \equiv 21 \equiv 10 \equiv -1 \mod 11$

$\therefore 7(-3) \equiv 1 \mod 11$

$\therefore [x] = [-3] = [8]$

Proposition: Let $a \in \mathbb{Z}$, $m \in \mathbb{N}$.

(a) $[a]^{-1}$ exists in $\mathbb{Z}_m$ iff $\gcd(a,m)=1$

(b) $[a]^{-1}$ is unique if it exists.

Pf: (a) $[a]^{-1}$ exists

$\iff [a][x]=[1]$ is solvable in $\mathbb{Z}_m$

$\iff ax+my=1$ is a solvable LDE

$\iff \gcd(a,m)=1$ (GCD 00)

(b) Assume $[a]^{-1}$ exists. Suppose $\exists$ $b \in \mathbb{Z}$ s.t. $[a][b]=[1]=[b][a]$.

Then $[a]^{-1}[a][b]=[a]^{-1}[1]$

$[1][b]=[a]^{-1}$

$[b]=[a]^{-1}$ ∎.

Practice problem: Solve $[15][x] + [7] = [12]$ in $\mathbb{Z}_{10}$.

The following are equivalent (TFAE)

- $a \equiv b \pmod{m}$
- $m \mid (a - b)$
- $\exists k \in \mathbb{Z}, a - b = km$
- $\exists k \in \mathbb{Z}, a = km + b$
- a and b have the same remainder when divided by m
- $[a] = [b]$ in $\mathbb{Z}_m$.

Theorem (LCT 2). *Let $a, c \in \mathbb{Z}$ and let $m \in \mathbb{N}$. Let $\gcd(a, m) = d$. The equation $[a][x] = [c]$ in $\mathbb{Z}_m$ has a solution if and only if $d \mid c$. Moreover, if $[x] = [x_0]$ is one particular solution, then the complete solution is*

$$\left\{[x_0], [x_0 + \tfrac{m}{d}], [x_0 + 2\tfrac{m}{d}], \ldots, [x_0 + (d-1)\tfrac{m}{d}]\right\}$$

Fermat's Little Theorem (FLT)

If p is a prime number and $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$. Equivalently, $[a^{p-1}] = [1]$ in $\mathbb{Z}_p$.

Ex: $5^6 \equiv 1 \bmod 7$, $4^6 \equiv 1 \bmod 7$, $39^6 \equiv 1 \bmod 7$

Note 1: $p-1$ is in the exponent! Note

$$6^3 \not\equiv 1 \bmod 7$$

Note 2: $p-1$ is not necessarily the smallest exponent s.t. $a^k \equiv 1 \bmod p$. Ex: $6^2 \equiv 1 \bmod 7$.

Lemma: Modulo p, the sets $S=\{a, 2a, \ldots (p-1)a\}$ & $T=\{1,2,\ldots p-1\}$ consist of the same elements provided $\gcd(a,p)=1$.

Pf: We show that S has $p-1$ distinct non zero elements modulo p. Let $1 \le k, m \le p-1$ be integers. Now if $ka \equiv ma \bmod p$ then $p \mid a(k-m)$. Since $\gcd(a,p)=1$, $p \mid (k-m)$ by CAD. Since $-p < 2-p \le k-m \le p-2 < p$ and $p \mid k-m$, we see that $k-m=0$ ie $k=m$.

Lastly, if $ka \equiv 0 \bmod p$ then $p \mid ka$. By Euclid's Lemma, $p \mid k$ (# $1 \le k \le p-1$ and p is prime) OR $p \mid a$ (# since $\gcd(a,p)=1$) Thus, S has $(p-1)$ distinct non zero elements modulo p. ∎.

Lemma proof recap:

(1) Start with $ka, ma \in S$

(2) Show $ka \equiv ma \bmod p \iff k = m$

(3) Show if $ka \in S$ is s.t. $ka \equiv 0 \bmod p$
then we have a contradiction.

Pf of FLT:

Using the lemma, valid since $p \nmid a \iff \gcd(a,p)=1$ (GCDPF), we have

$$\underbrace{\prod_{k=1}^{p-1} ka}_{\text{product of elets of } S} \equiv \underbrace{\prod_{k=1}^{p-1} k}_{\text{product of elets. of } T.} \pmod p$$

Let $Q = \prod_{k=1}^{p-1} k = (1)(2)\cdots(p-1)$. Then

$$Q a^{p-1} \equiv Q \pmod p$$

Since $\gcd(Q,p)=1$ ($\because Q$ is a product of terms less than a prime p), Q^{-1} exists hence

$$Q^{-1} Q a^{p-1} \equiv Q^{-1} Q \pmod p$$

$$a^{p-1} \equiv 1 \pmod p. \quad \blacksquare$$