$m = 14$ Inverses?

$\mathbb{Z}_{14} = \{0, 1, 2, 3, \ldots, 13\}$

$49 = 3 \cdot 14 + 7$

$7 \times 7 = 7^2 = 7$ example

additive inverse of a would be $-a$,

$14 - a \equiv_{14} -a$ So additive inverse of a is $14-a$.

Check $a + (14-a) = 0$

↑ between 0 and 13

$3 + 11 = 0$

14 is even

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13

additive inverses

$-13 = 1$

$13 = -1$

$7+7 = 0$, $0+0 = 0$

multiplication in $\mathbb{Z}_{14}$ $1 \times 1 = 1$

$3 \times 5 = 1$ ← 3 and 5 are mult. inverses.

5×3

" $\frac{1}{3} = 5$ in $\mathbb{Z}_{14}$ "

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13

$9 \times 11 = 1$

$13 \times 13 = 1$

$(-1) \times (-1) = 1$

1, 15, 29, 43, 57, 71, 85, 99

↑ remainder of 1 and dividing by 14

$12 = 2 \times 6$ $\gcd(12, 14) = 2$

Conclude 12 has no m.i. ← try mult. 12 times everything.

$7 \times 12 = 14 \cdot 6 = 0$

Suppose $12a = 1$ then $7 \times (12a) = 7$

$(7 \times 12) \times a$

$0 \times a = 0$

but $7 \neq 0$ in $\mathbb{Z}_{14}$

a	$12 \times a$
0	0
1	12
2	10
3	8
4	6
5	4
	.
	.
	.
	1
	.

← look for 1's

$36 = 2 \times 14 + 8$

60

$56 + 4$

In $\mathbb{Z}_5$ the equation $x^2 + 1 = 0$ has a solution.

$2^2 + 1 = 0$

x	$x^2 + 1$
0	1
1	2
2	0 ←
3	0 ←
4	2

$x^2 + 1 = 0$ has 2 solutions.