Lesson 23

Inverses in $\mathbb{Z}_m$

Recall $\mathbb{Z}_m = \{ [0]_m, [1]_m, \cdots [m-1]_m \}$

We write $\mathbb{Z}_m = \{0, 1, \cdots m-1\}$

Def $a \in \mathbb{Z}_m$ is invertible iff there is an element in $\mathbb{Z}_m$ which we call the inverse of a and denote by a^{-1} s.t $a \cdot a^{-1} = 1$ in $\mathbb{Z}_m$ that is $a \cdot a^{-1} \equiv_m 1$

Note : a is invertible in $\mathbb{Z}_m$ iff $ax \equiv_m 1$ has solution

Th a is invertible in $\mathbb{Z}_m \iff (a, m) = 1$

Example : what are the invertible elements of $\mathbb{Z}_4 = \{0, 1, 2, 3\}$?

1 and 3 since $(1, 4) = 1$ $(3, 4) = 1$

but $(0, 4) = 4 \neq 1$ and $(2, 4) = 2 \neq 1$

$1^{-1} = 1$ since $1 \cdot 1 = 1$ in $\mathbb{Z}_4$

$3^{-1} = 3$ since $3 \cdot 3 = 1$ in $\mathbb{Z}_4$

Example what are the invertible elements of $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$?

1 ; $1^{-1} = \underline{1}$

2 ; $2^{-1} = 3$

3 ; $3^{-1} = 2$

4 ; $4^{-1} = 4$

Note if p is prime, every non zero element of $\mathbb{Z}_p$ is invertible.

Solve $3x \equiv 4 \mod 5$

$3x \equiv_5 4 \iff 3^{-1} \cdot 3x \equiv_5 3^{-1} 4$

(since (5, any invertible element) = 1

$\iff x \equiv_5 2 \cdot 4 \equiv_5 3$

Note in Z_p for p prime, if $a \cdot b = 0$
and $a \neq 0$ then a^{-1} exists so
$a^{-1} a b = 0$ so $b = 0$
So in Z_p if $ab = 0$ $a = 0$ or $b = 0$

Let g $Z_4 \longrightarrow Z_4$
$f(x) = 3 \cdot x$

Then
$f(0) = 0$
$f(1) = 3$
$f(2) = 2$
$f(3) = 1$

I can see g is a bijection

Now consider $f \quad \mathbb{Z}_{40} \to \mathbb{Z}_{40}$

$f(x) = 3 \cdot x$

f is injective : proof

assume $f(x_1) = f(x_2)$ this means

$3x_1 \equiv_{40} 3x_2$ and using

the cancellation law, since $(3, 40) = 1$

we have $x_1 \equiv_{40} x_2$ or

$x_1 = x_2$ in $\mathbb{Z}_{40}$

f is surjective : proof

Given $y \in \mathbb{Z}_{40}$ I want to find

$x \in \mathbb{Z}_{40}$ s.t $3x = y$ in $\mathbb{Z}_{40}$

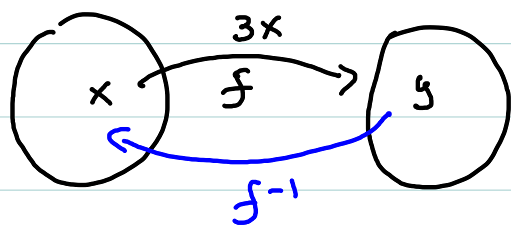
that is $3x \equiv_{40} y$

This linear congruence has solutions

since $(3, 40) = 1$.

f is then a bijection. Can you define f^{-1} ?

$f^{-1} \quad \mathbb{Z}_{40} \to \mathbb{Z}_{40}$



$y = 3x \qquad x = 3^{-1} y$ here 3^{-1}
is the inverse of 3 in $\mathbb{Z}_{40}$ so
3^{-1} is the solution to $3x \equiv_{40} 1$

$3X \equiv 1 \mod 40$

Associate diophantine equation
$3x + 40y = 1$

1) compute $(40, 3)$

$$40 = 3 \cdot 13 + 1$$
$$3 = 1 \cdot 3 + 0$$

2) $1 = 3(-13) + 40$

3) Sol in $\mathbb{Z}_{40}$ is $x = -13 + 40 = 27$

Therefore $f^{-1}\ \mathbb{Z}_{40} \to \mathbb{Z}_{40}$
$f^{-1}(y) = 27y$

Check $f^{-1}(f(x)) = \underbrace{27 \cdot 3}_{81} \cdot X = X$

$f(f^{-1}(y)) = 3 \cdot 27 y = y$

Th: Consider $f \; \mathbb{Z}_m \to \mathbb{Z}_m$
$f(x) = ax$

if $(a, m) = 1$ then f is a bijection.

Proof:

f is injective: assume $ax_1 = ax_2$ in $\mathbb{Z}_m$

that is $ax_1 \equiv ax_2 \mod m$, then

$x_1 \equiv x_2 \mod \frac{m}{1}$ so $x_1 = x_2$ in $\mathbb{Z}_m$

f is surjective: given y in $\mathbb{Z}_m$

the congruence $ax \equiv y \mod m$ has a

solution $\cdot x_1$ since $(a, m) = 1$ divides y

then $f(x_1) = y$ in $\mathbb{Z}_m$

Question: what can we say about

$f\ \mathbb{Z}_m \to \mathbb{Z}_m$
$f(x) = ax$ if $(a, m) = d > 1$?

Is f still a bijection (for all a, m)
sometimes a bijection?
Never a bijection?