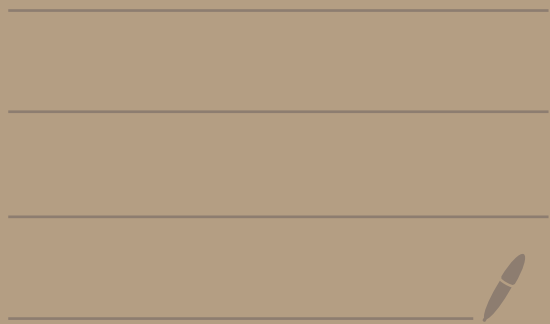


Math 4460

4/10/23



Question: When is an element of \mathbb{Z}_n^\times equal to its multiplicative inverse?

We will answer this when n is a prime.

Ex: $n = 7$

$$\mathbb{Z}_7^\times = \{ \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6} \}$$

$$\bar{1} \cdot \bar{1} = \bar{1}$$

$$\bar{1}^{-1} = \bar{1}$$

$$\bar{2} \cdot \bar{4} = \bar{8} = \bar{1}$$

$$\begin{aligned} \bar{2}^{-1} &= \bar{4} \\ \bar{4}^{-1} &= \bar{2} \end{aligned}$$

$$\bar{3} \cdot \bar{5} = \bar{15} = \bar{1}$$

$$\begin{aligned} \bar{3}^{-1} &= \bar{5} \\ \bar{5}^{-1} &= \bar{3} \end{aligned}$$

$$\bar{6} \cdot \bar{6} = \bar{36} = \bar{1}$$

$$\bar{6}^{-1} = \bar{6}$$

$$[36 - 1 = 35 = 7 \cdot 5 \mid 36 \equiv 1 \pmod{7}]$$

So, $\bar{1}$ and $\bar{6}$ are equal to their own multiplicative inverses.

Note: $\bar{6} = \overline{-1}$ in \mathbb{Z}_7

Theorem: Let p be a prime.

If $\bar{x} \in \mathbb{Z}_p^x$ and $\bar{x}^2 = \bar{1}$,

then $\bar{x} = \bar{1}$ or $\bar{x} = \overline{p-1} = \overline{-1}$

That is, the only elements of \mathbb{Z}_p^x that are equal to their multiplicative inverse are

$\bar{1}$ and $\overline{p-1} = \overline{-1}$.

Proof: Let $\bar{x} \in \mathbb{Z}_p^x$ where

$$\overline{x}^2 = \overline{1}. \quad [\text{Here } x \in \mathbb{Z}]$$

Then $x^2 \equiv 1 \pmod{p}$.

So, $p \mid (x^2 - 1)$.

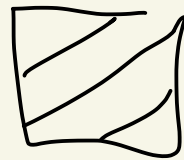
Thus, $p \mid (x+1)(x-1)$.

So, $p \mid (x+1)$ or $p \mid (x-1)$.

Hence, $x \equiv -1 \pmod{p}$

or $x \equiv 1 \pmod{p}$.

Ergo, $\overline{x} = \overline{-1} = \overline{p-1}$ or $\overline{x} = \overline{1}$.



p Prime
If $p \mid ab$
then
 $p \mid a$ or
 $p \mid b$

Note: The theorem may not be true if n is not prime

For example, last Weds

We saw that

$$\mathbb{Z}_{15}^{\times} = \{ \bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14} \}$$

and

$\bar{1}^{-1} = \bar{1}$	$\bar{7}^{-1} = \bar{13}$	$\bar{13}^{-1} = \bar{7}$
$\bar{2}^{-1} = \bar{8}$	$\bar{8}^{-1} = \bar{2}$	$\bar{14}^{-1} = \bar{14}$
$\bar{4}^{-1} = \bar{4}$	$\bar{11}^{-1} = \bar{11}$	

Here we have 4 elements that are their own multiplicative inverse. They are $\bar{1}, \bar{4}, \bar{11}, \bar{14}$.

Ex: Let's illustrate the next theorem (Wilson's theorem) with $p=13$.

Note 13 is prime.

Check out what happens when you multiply all the elements of \mathbb{Z}_{13}^{\times} together.

$$\begin{aligned} \overline{12!} &= \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \overline{6} \cdot \overline{7} \cdot \overline{8} \cdot \overline{9} \cdot \overline{10} \cdot \overline{11} \cdot \overline{12} \\ &= \overline{1} \cdot \underbrace{(\overline{2} \cdot \overline{7})}_{\text{these are inverses}} \underbrace{(\overline{3} \cdot \overline{9})}_{\text{these are inverses}} \underbrace{(\overline{4} \cdot \overline{10})}_{\text{these are inverses}} \underbrace{(\overline{5} \cdot \overline{8})}_{\text{these are inverses}} \underbrace{(\overline{6} \cdot \overline{11})}_{\text{these are inverses}} \cdot \overline{12} \end{aligned}$$

these are their own inverse

$$= \overline{1} \cdot \overline{14} \cdot \overline{27} \cdot \overline{40} \cdot \overline{40} \cdot \overline{66} \cdot \overline{12}$$

$$= \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{12}$$

$$= \overline{12} = \overline{-1}$$

↑

$12 \equiv -1 \pmod{13}$

$$\overline{14} = \overline{1}$$

$$\overline{27} = \overline{1}$$

$$\overline{40} = \overline{1}$$

$$\overline{66} = \overline{1}$$

multiples
of 13

13

26

39

52

65

⋮

So,

$$\overline{12!} = \overline{12} = \overline{-1}.$$

Theorem (Wilson's Theorem)

Let p be a prime.

Then, $\overline{(p-1)!} = \overline{p-1} = \overline{-1}$ in \mathbb{Z}_p^x .

proof:

If $p=2$, then

$$\overline{(p-1)!} = \overline{1!} = \overline{1} = \overline{p-1}.$$

Now assume $p > 2$.

So, p is an odd prime.

Recall $\mathbb{Z}_p^x = \{ \overline{1}, \overline{2}, \overline{3}, \dots, \overline{p-2}, \overline{p-1} \}$

these each have
an inverse not
equal to them

one their own
inverses

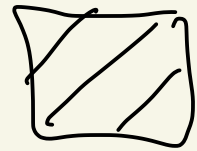
So,

$$\overline{(p-1)!} = \overline{1 \cdot 2 \cdot 3 \cdots (p-2)(p-1)}$$

every element
in this range
cancels with
its inverse

$$= \overline{1} \cdot \overline{p-1}$$

$$= \overline{p-1} = \overline{-1}$$



HW 3

②(b) Show that $\sqrt{6}$ is irrational.

Proof:

Suppose to the contrary that $\sqrt{6}$ was rational.

Then, $\sqrt{6} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$,

$b \neq 0$ and $\gcd(a, b) = 1$.

From HW 3 #1(a)

Hence, $6 = \frac{a^2}{b^2}$.

Then, $6b^2 = a^2$

So, $2 \cdot 3 \cdot b^2 = a^2$.

$\uparrow \uparrow$
pick one

6 is not prime. We need a prime so we can use its magical powers

Let's use 3.

The above says $3(2b^2) = a^2$.

So, $3 \mid a^2$.

Since 3 is prime and $3 \mid a \cdot a$,

so $3 \mid a$.

$p \mid xy \rightarrow p \mid x$ or $p \mid y$
 $[p \text{ prime}]$

Thus, $a = 3k$
where $k \in \mathbb{Z}$.

Plug this back into $2 \cdot 3 \cdot b^2 = a^2$
to get $2 \cdot 3 \cdot b^2 = 3^2 k^2$.

Divide by 3 to get $2b^2 = 3k^2$.

So, $3 \mid 2b^2$.

Since 3 is prime, $3 \mid 2$ or $3 \mid b^2$.

can't happen

Since $3 \nmid 2$ we know $3 \mid b^2$.

Since 3 is prime and $3 \mid b \cdot b$

we know $3 \mid b$.

Since $3 \mid a$ and $3 \mid b$ we

have $\gcd(a, b) \geq 3$

which contradicts

$\gcd(a, b) = 1$.

Thus, $\sqrt{6}$ is irrational.

