Math 4460
4/10/23

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

We will answer this when n is a prime.

Ex: $n = 7$

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

$\overline{1} \cdot \overline{1} = \overline{1}$ ← $\boxed{\overline{1}^{-1} = \overline{1}}$

$\overline{2} \cdot \overline{4} = \overline{8} = \overline{1}$ ← $\boxed{\overline{2}^{-1} = \overline{4} \quad \overline{4}^{-1} = \overline{2}}$

$\overline{3} \cdot \overline{5} = \overline{15} = \overline{1}$ ← $\boxed{\overline{3}^{-1} = \overline{5} \quad \overline{5}^{-1} = \overline{3}}$

$\overline{6} \cdot \overline{6} = \overline{36} = \overline{1}$ ← $\boxed{\overline{6}^{-1} = \overline{6}}$

$36 - 1 = 35 = 7 \cdot 5$ | $36 \equiv 1 \pmod 7$

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

$\boxed{\underline{\text{Note:}}\ \overline{6} = \overline{-1} \text{ in } \mathbb{Z}_7}$

<u>Theorem:</u> Let p be a prime. If $\overline{x} \in \mathbb{Z}_p^{\times}$ and $\overline{x}^2 = \overline{1}$, then $\overline{x} = \overline{1}$ or $\overline{x} = \overline{p-1} = \overline{-1}$

That is, the only elements of $\mathbb{Z}_p^{\times}$ that are equal to their multiplicative inverse are $\overline{1}$ and $\overline{p-1} = \overline{-1}$.

<u>proof:</u> Let $\overline{x} \in \mathbb{Z}_p^{\times}$ where

$\overline{x}^2 = \overline{1}$. [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 $p \mid (x-1)$.

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

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

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

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

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

For example, last Weds we saw that

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

and

$$\overline{1}^{-1} = \overline{1} \qquad \overline{7}^{-1} = \overline{13} \qquad \overline{13}^{-1} = \overline{7}$$

$$\overline{2}^{-1} = \overline{8} \qquad \overline{8}^{-1} = \overline{2} \qquad \overline{14}^{-1} = \overline{14}$$

$$\overline{4}^{-1} = \overline{4} \qquad \overline{11}^{-1} = \overline{11}$$

Here we have 4 elements that are their own multiplicative inverse

They are $\overline{1}, \overline{4}, \overline{11}, \overline{14}$.

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.

$$\overline{12}! = \overline{1}\cdot\overline{2}\cdot\overline{3}\cdot\overline{4}\cdot\overline{5}\cdot\overline{6}\cdot\overline{7}\cdot\overline{8}\cdot\overline{9}\cdot\overline{10}\cdot\overline{11}\cdot\overline{12}$$

$$= \underbrace{\overline{1}}\cdot\underbrace{(\overline{2}\cdot\overline{7})}\underbrace{(\overline{3}\cdot\overline{9})}\underbrace{(\overline{4}\cdot\overline{10})}\underbrace{(\overline{5}\cdot\overline{8})}\underbrace{(\overline{6}\cdot\overline{11})}\cdot\underbrace{\overline{12}}$$

these are inverses

these are their own inverse

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

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

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

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

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

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

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

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

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 $\mathbb{Z}_p^\times$.

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 $\mathbb{Z}_p^\times = \{\overline{1}, \underbrace{\overline{2}, \overline{3}, \ldots, \overline{p-2}}_{\text{these each have an inverse not equal to them}}, \overline{p-1}\}$

are their own inverses

So,

$$\overline{(p-1)!} = \overline{1}\cdot\underbrace{\overline{2}\cdot\overline{3}\cdot\cdots\cdots(\overline{p-2})}_{\text{every element in this range cancels with its inverse}}(\overline{p-1})$$

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

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

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 $\underbrace{\gcd(a,b) = 1}_{\text{From Hw 3 \#1(a)}}$.

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

Then, $\boxed{6b^2 = a^2}$

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

So, $\underbrace{2 \cdot 3}_{\text{pick one}} \cdot b^2 = a^2$.

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 $\boxed{3 \mid a.}$

$p \mid xy \to p \mid x$ or $p \mid y$

$\boxed{p \text{ prime}}$

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, $\underbrace{3 \mid 2}_{\text{can't happen}}$ or $3 \mid b^2$.

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

Since 3 is prime and $3 \mid b \cdot b$ we know $\boxed{3 \mid b.}$

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. $\blacksquare$