* Method #2: By the "multiplication" interpretation

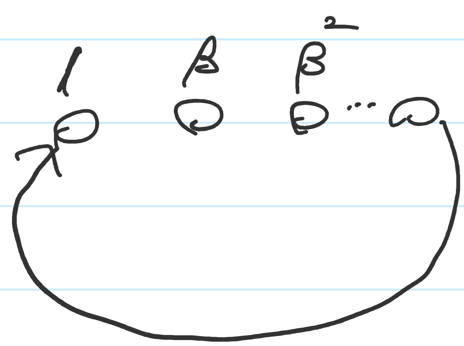
* Need new definitions:

- For any $\beta \in GF(p) \setminus \{0\}$

  $1, \beta, \beta^2, \cdots$ must eventually <u>repeat</u>.

  Since $GF(p)$ is finite.

- Furthermore, when it repeats, it must reach 1 first



pf: If $\beta^3 = \beta^m$

then $1 = \beta^{m-3}$

- Define the "<u>period</u>" of the repetition by m, we thus have

$$\underbrace{1=\beta^0, \beta^1, \beta^2, \cdots, \beta^{m-1}}_{m \text{ of them}}$$

$\underbrace{\qquad\qquad\qquad\qquad}_{m \text{ of them}}$

- Define the m value of β as the <u>order</u> of β. Sometimes written as $\mathrm{ord}(\beta)$.
- m is the smallest integer such that $\beta^m = 1$
- Note that $\{1, \beta, \ldots, \beta^{m-1}\}$ is a commutative subgroup of $GF(p) \setminus \{0\}$
- By Lagrange Theorem

$$\boxed{\frac{p-1}{m} \text{ must be an integer}}$$

- This also means $\boxed{\beta^{p-1} = 1}$

since $\beta^m = 1$

- An element β is <u>primitive</u> if

$\mathrm{ord}(\beta) = p-1$, that is

$$\underbrace{1, \beta, \beta^2, \cdots, \beta^{p-2}}_{p-1 \text{ of them}}$$ will cycle

through the entire set $GF(p) \setminus \{0\}$

* Equivalently, β is primitive if it is a <u>generator</u> of the multiplicative group $GF(p) \setminus \{0\}$ of the field.

☆ We can thus represent a finite field by

$$GF(p) = \{0, 1, \beta^1, \beta^2, \cdots, \beta^{p-2}\}$$

by any <u>primitive</u> element β.

* Further more

$$\beta^i \cdot \beta^j = \beta^{i+j} = \beta^{\mathrm{mod}(i+j,\, p-1)}$$

$$\beta^{i} \cdot \beta^{j} = \beta^{i+j} = \beta^{\mathrm{mod}(i+j,\, p-1)}$$

is (relatively) easy to compute.

E.g. $p=7$.

$GF(7) = \{0, 1, \cdots, 6\}$

$1, 2, 4, 8=1, \ldots$ $\quad \mathrm{ord}(2) = 3$

$1, 3, 9=2, 6, 4, 5, 1$ $\quad \mathrm{order}(3) = 6$

$1, 4, 2, 1, \ldots$ $\quad \mathrm{ord}(4) = 3$

$1, 5, 4, 6, 2, 3, 1$ $\quad \mathrm{ord}(5) = 6$

$1, 6, 1, 6, \ldots$ $\quad \mathrm{ord}(6) = 2$

$\Rightarrow$ We can choose either $\beta=3$ or $\beta=5$

E.g. [illegible] $\beta=5$.

$GF(7) = \{0, 1, \beta^1 = 5, \beta^2 = 4, \beta^3 = 6, \beta^4 = 2,$
$\beta^5 = 3\}$

E.g. $\beta^3 \cdot \beta^5 \cdot \beta^2 = \beta^{10} = \beta^{\mathrm{mod}(10, 7-1)}$
$= \beta^4$

Q: For any p, do we always have a <u>primitive</u> element?

Ans: Yes, the number of primitive elements is the number of $1 \leq x \leq p-1$ such that <u>x</u> and <u>$p-1$</u> are <u>co-prime</u>

i.e. $g.c.d(x, p-1) = 1$

E.g. $p = 7$, $p - 1 = 6$ there are two numbers 1, and 5 that are <u>co-prime</u> to 6. Note that

- 1 and 5 in integers are co-prime to 6

- $\beta=3$, $\beta=5$ in $GF(7)$ are the primitive elements

- There is no easy relationship between the co-prime values in integer and the primitive elements in $GF(p)$, except that their numbers are identical.

Summary: $GF(p)$ p is a prime can be defined by the modulo p operations, and we can either represent it by

$$GF(p)=\{0,1,2,\cdots,p-1\}$$

or by $GF(p)=\{0,1,\beta,\beta^2,\cdots,\beta^{p-2}\}$

for any primitive β.