Powers of Elements

Eg $\{2,4,6,8\}$ under mult mod 10

	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

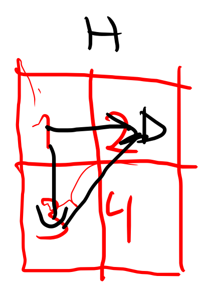
elt	order (elt)
2	4
4	2
6	1
8	4

$\mathbb{Z}_4$

Checkerboard Game.

	I	V	H	D
I	I	V	H	D
V	V	I	D	H
H	H	D	I	V
D	D	H	V	I

elt	order
I	1
V	2
H	2
D	2



V

V_4

① Order of a Group: $|G|$

Number of elts in a group.

② Def^n: The order of an element x in a group G, denoted $|x|$;

- is said to be finite if $x^n = e$ for some $n > 0$, choose the least such n as the order of the element
- if no such n exists the it has infinite order.

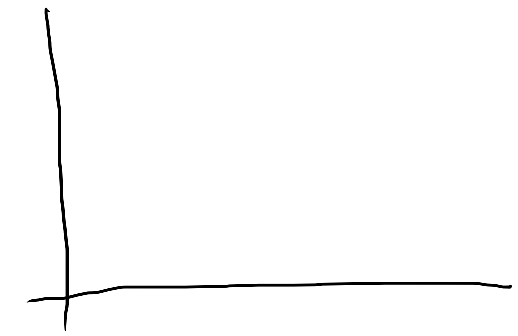
$G = (\mathbb{Z}, +)$: $|1| = \infty$: $1+1=2$, $2+1=3$, $3+1=4$ ...

$|0| = 1$: $0=0$

Fact: $|e| = 1$ in any group. $e^1 = e$

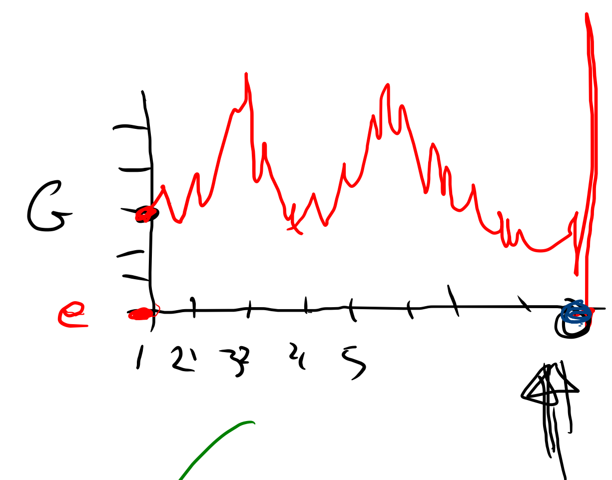
Thm 16: Finite Group.
p. 44

a) powers cannot all be different
b) there is a smallest k, pos. integer, s.t $x^k = e$.
This $k = |x|$.



Thm 1. Let x be an elt of a finite group, G.
Then the powers of x cannot be all different.

Proof: Since the group is finite there only a finite number of values the powers of x can take.
- Since there are only a finite in the infinite sequen, some values must repeat by the PHP.



Thm: 2. Let x be an elt of a finite group G,
Then there is a smallest pos. integer s.t. $x^k = e$. ← Return e

Consider all consequtive powers of an elt x

$x^1 \; x^2 \; x^3, \ldots$

- at some point in the sequence we will get a ~~two~~ repetition
- So $x^r = x^s$
$r \neq s$ choose $r < s$

$x^r = x^s$

$x^{-r} x^r = x^{-r} x^s$

$\boxed{e = x^{s-r}}$

We know $s > r$

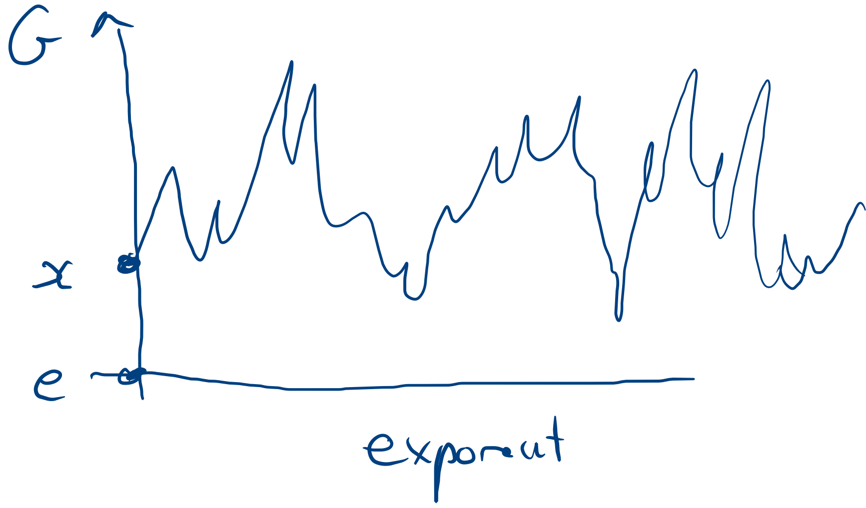
By WOP there is a minimum such $s - r \equiv k$ exist.

2. Summary: ① Infinite order elt:

$x^N = e$ iff $N=0$ ← no return to e.

→ ② finite order elt of n,

$x^N = e$ iff $n \mid N$



1.) Let $x \in G$ have infinite order & N is an integer.

$\boxed{\text{Then } x^N = e \text{ iff } N = 0.}$

If: If $N=0 \implies x^N = e$.

Pf If $N=0$ then $x^N = x^0 = e$ by def$^{\Delta}$.

Of: If $x^N = e$ then $N=0$.

Pf: Since it's ∞ order elt, then by def^n. N cannot be >0.

$\therefore N \le 0$.

But if $x^N = e \longrightarrow x^{-N} = (x^N)^{-1} = e^{-1} = e$

$x^{-N} = e$

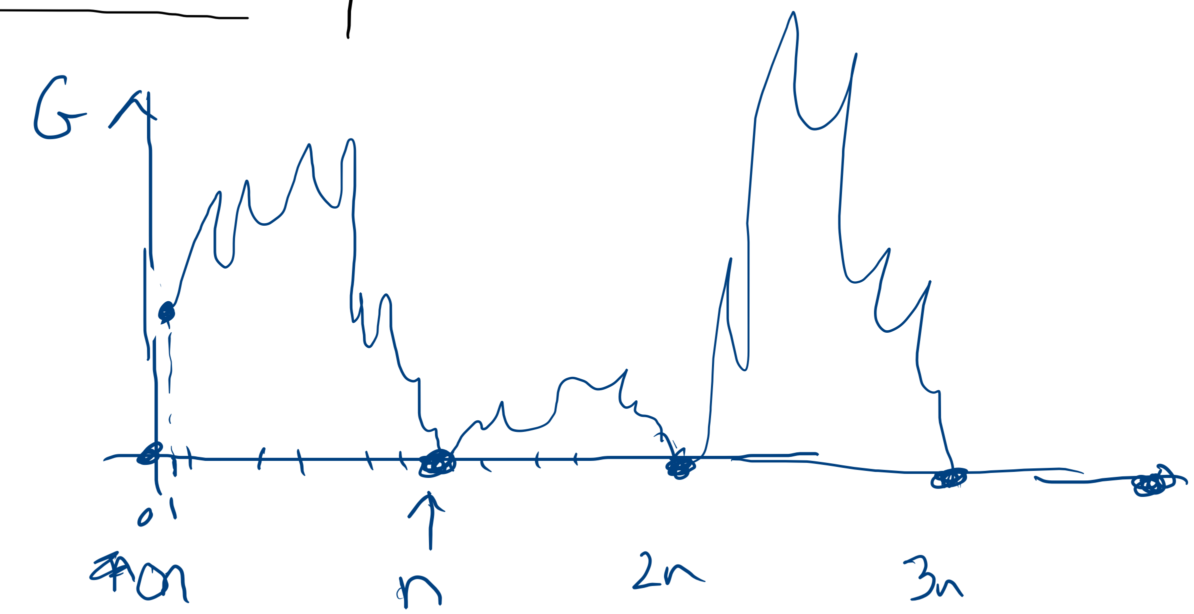
$\therefore$ N cannot be < 0 either.

$\therefore$ $\boxed{N = 0.}$

2. Let x have a finite order n & let N be an integer. Then $x^N = e$ iff n divides into N, i.e, $n \mid N$.

E.g. $n = 3$

$x^N = e \Rightarrow 0, 3, 6, -3, -9, \dots$



Proof: $\Leftarrow$ If: If $n \mid N \longrightarrow x^N = e$.

Proof If $n \mid N$ then $N = n \cdot s$ for $s \in \mathbb{Z}$

$$x^N = x^{n \cdot s} = (x^n)^s = e^s$$

$$\boxed{x^N = e}$$

$\rightarrow$ Pf: If $x^N = e$ then $n \mid N$

Proof: If $x^N = e \rightarrow$ and we can always write $\boxed{N = qn + r}$ where $0 \leq r < n$.

$$x^N = x^{qn+r} = (x^n)^q \cdot x^r$$

e

$\boxed{x^N = x^r}$ c $0 \leq r < n$

$\boxed{e = x^r} \rightarrow \therefore r = 0$

$n = 5$

$x^0 = e$

$x^1 = x$

x^2

$\vdots$

$x^5 = e$

$\rightarrow$ But if $r = 0$ then $N = qn + 0$

$\therefore N = qn.$

Which mean $n \mid N$.

Th^{m}: $\boxed{\text{If an elt has finite order, } n\text{, then } \underline{x^r = x^s} \text{ iff } \underline{r \equiv s \pmod n}\text{, so powers repeat consecutively in cycles of length } n.}$

Proof: If $\Leftarrow$: If $r \equiv s \pmod n$ then $\underline{x^r = s^s}$.

$\Rightarrow$ If $r \equiv s \pmod n$, then $\underline{s = kn + r}$

$$\therefore x^s = x^{kn+r}$$

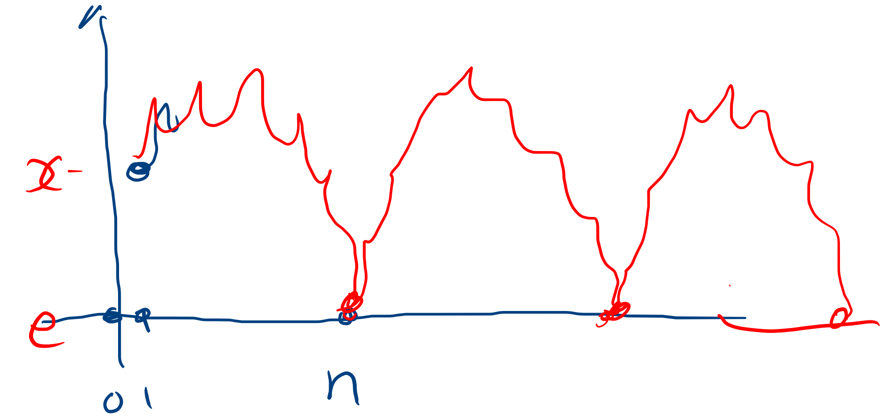
$$= \cancel{(x^n)^k}\, x^r$$

$$\boxed{x^s = x^r}$$

Of: $\rightarrow$ If $\underline{x^r = x^s} = x^{r-s} = e$

$$\therefore n \mid r-s$$

$$\therefore \boxed{r \equiv s \bmod n.}$$



$\underline{2} \equiv \underline{17} \pmod{\underline{5}}$

$17 = k \cdot 5 + 2$

$x^N = e \Rightarrow n \mid N.$

$5 \mid 17 - 2.$