$a \in G$

$\text{ord}\, a \mid |G|$

if $|G|$ – is a prime number,

$\text{ord}\, a \in \{1, |G|\}$

the $\text{ord}\, a = 1 \Rightarrow a = \mathcal{O}$

$a + a + \dots + a = \mathcal{O}$

ord a – minimal number of occurrences of a here

So if $a \neq \mathcal{O} \Rightarrow \text{ord}\, a = |G|$

$\langle a \rangle = G$ ☺

---

So how to generate an instance for the ~~task~~ L2?

use the sage script: $P$, $E_{a,b}(\mathbb{F}_p)$, $\mathcal{O}$

$\mathcal{O} = (x, y, 1) \to (x, y)$

projective normative affine

$\text{ord}\, P = \#E_{a,b}(\mathbb{F}_p)$

is prime

let us call it $q$

Let $s$ be a random element of

$\{2, 3, \dots, q-1\}$

and generate:

$Y = s \cdot P$

ord P

Pollard-$\rho(Y, P, q, p, a, b)$

basepoint

necessary to define the arithmetic

$s'$

if $s' = s \pmod q$ ? $Y = s \cdot P$ alternatively

---

Pollard-$\rho$ : we search for a collision between $T = H$ ?

Can we take advantage of the fact that $T$ and $-T$ ~~(H and -H)~~ have the same x coordinate?