1.6 Groups and El Gamal cryptosystems.

Def A structure $(G, *)$ with one binary operation $* : G \times G \to G$ is called a group, if the following are true: There exists $e \in G$ such that for every $a \in G$ one has $e * a = a * e = a$. [e is a so-called neutral element and it is necessarily unique.];

For every $a \in G$ there exists $b \in G$ such that $a * b = b * a = e$ [this b is uniquely determined by a and is called the inverse of a; notation: $b = a^{-1}$.];

For every $a, b, c \in G$ one has $a * (b * c) = (a * b) * c$.

A group is called Abelian or commutative if, additionally, $a * b = b * a$ holds for every $a, b \in G$.

Examples If $(R, +, \cdot)$ is a commutative ring, then $(R, +)$ is an Abelian group.

$(R, \cdot)$ is not a group, but $(R^\times, \cdot)$ is an Abelian group.

$R^\times$: the set of units.

In particular, if R is a field, then $(R \setminus \{0\}, \cdot)$ is an Abelian group.

Notation If $(G, *)$ is a group and $g \in G$, $k \in \mathbb{Z}$, then we can raise g to the power k. This is defined as follows:

$$g^k := \begin{cases} \underbrace{g * \dots * g}_{k \text{ times}} & \text{if } k > 0 \\ e & \text{if } k = 0 \\ \underbrace{g^{-1} * \dots * g^{-1}}_{-k \text{ times}} & \text{if } k < 0 \end{cases}$$

If we fix k, we have the power function $g \in G \mapsto g^k \in G$.

If we fix g and change k, we have the exponential function $k \in \mathbb{Z} \longmapsto g^k \in G$. El Gamal encryption systems use the exponential function.

Some more Notation

Sometimes, the group operation is denoted as $\cdot$ and one uses the multiplicative terminology (the neutral element is denoted as 1 then).

For Abelian groups, one sometimes denotes the group operation as $+$ and uses the additive terminology: 0 neutral element; $-a$ additive inverse of a; $3a = a+a+a$, $-4a = (-a)+(-a)+(-a)+(-a)$ etc.

Proposition 12 Let $(G, *)$ be a group of finite size $|G| < \infty$. Then for every $g \in G$ there exists some $n \in \mathbb{N}$ such that $g^n = e$. Furthermore, if n is the minimal number with this property, then the elements

$g^0, g^1, \dots, g^{n-1}$ are pairwise distinct.

Proof. Consider the infinite sequence $g^0, g^1, g^2, \dots$

The members of this sequence belong to the finite set G.

So, there are $i, j \in \mathbb{N}_0$ with $i < j$ such that $g^i = g^j$.

$\Rightarrow e = g^{-i} g^i = g^{-i} \cdot g^j = g^{j-i}$ So, the assertion is true for $n = j - i$. Now, consider the minimal $n \in \mathbb{N}_0$ such that $g^n = e$. We need to check that $g^0, \dots, g^{n-1}$ are n distinct elements. Assume, that was not true and we had $0 \le i < j < n$ with $g^i = g^j$. But then we would have

$g^{j-i} = e$, where $0 \le j - i < n$, which is a contradiction to the choice of n. □

Def. If $(G, *)$ is a finite group and $g \in G$, then the minimal $n \in \mathbb{N}$ such that $g^n = e$ is called the order of g. Notation: $\operatorname{ord}(g)$.

Example

- $(\mathbb{Z}_6, +)$

$\operatorname{ord}([0]) = 1$

$\operatorname{ord}([1]) = 6$

$\operatorname{ord}([2]) = 3$

$\operatorname{ord}([3]) = 2$

$\operatorname{ord}([4]) = 3$

$\operatorname{ord}([5]) = 6$

$[2], \underbrace{2\cdot[2]}_{[0]}, \underbrace{3\cdot[2]}_{[0]}$

$[4], \underbrace{2\cdot[4]}_{[0]}, \underbrace{3\cdot[4]}_{[0]}$

- $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$

$\operatorname{ord}([1]) = 1$

$\operatorname{ord}([2]) = 4$

$\operatorname{ord}([3]) = 4$

$\operatorname{ord}([4]) = 2$

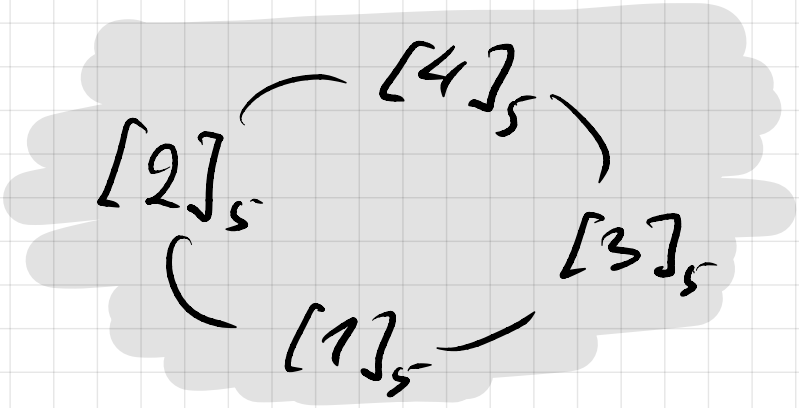
$[1]^1 = [1]$

$[2]^1, [2]^2 = [4], [2]^3 = [3], [2]^4 = [1]$

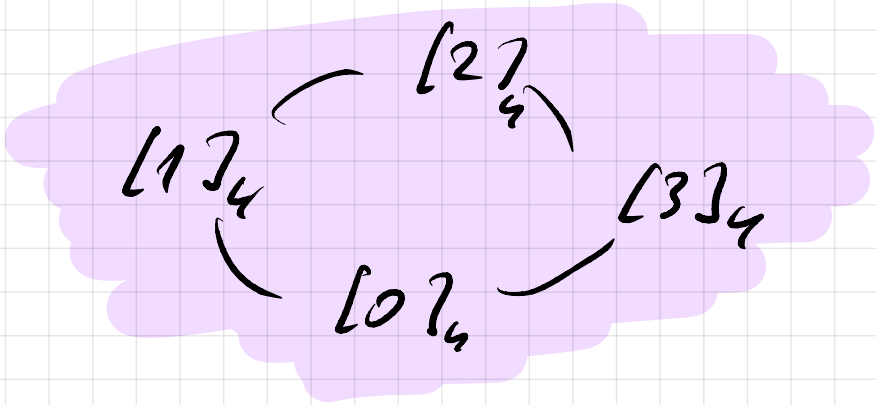
$[3]^1, [3]^2 = [4], [3]^3 = [2], [3]^4 = [1]$

$[4]^1, [4]^2 = [1]$

Interestingly $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ is pretty much the same thing as $(\mathbb{Z}_4, +)$.



$(\mathbb{Z}_5 \setminus \{0\}, \cdot)$



$(\mathbb{Z}_4, +)$

- $(\mathbb{Z}_8^\times, \cdot)$ $\quad \mathbb{Z}_8^\times = \{[1], [3], [5], [7]\}$

$\text{ord}([1]) = 1$

$\text{ord}([3]) = 2$

$\text{ord}([5]) = 2$

$\text{ord}([7]) = 2$

Computational question

Assume g is an element of order $n \in \mathbb{N}$ in a finite group G. Is it computationally hard to solve the equation $g^t = h$ in the unknown $t = 0, \ldots, n-1$?

Answer: it depends on the group and how it is given.

Example $(\mathbb{Z}_{100}, +)$

$\operatorname{ord}([21]) = 100$

$t \cdot [21] = [73]$

$t = 0, \dots, 99$ unknown.