Def: Grupa G se nazývá **CYKLICKÁ**, pokud $G = \langle a \rangle_G$ pro nějaké $a \in G$.

Věta: Buď G cyklická. Je-li G nekonečná, pak $G \simeq \mathbb{Z}$.
Je-li $|G| = n < \infty$, pak $G \simeq \mathbb{Z}_n$.

[KLASIFIKACE CYKLICKÝCH GRUP]

Věta: Buď G abelovská grupa s konečně mnoha generátory.
Pak $G \simeq \mathbb{Z}^n \times \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_m^{k_m}}$ pro nějaká $n, k_1, \dots, k_m \in \mathbb{N} \cup \{0\}$
$p_1, \dots, p_m$ prvočísla.

[KLASIFIKACE KONEČNĚ GENER. ABEL. GRUP]

Tvrzení (vlastnosti cyklických grup): Buď $G = \langle a \rangle$ cyklická, $|G| = n$.

(1) Podgrupy G jsou cyklické.

(2) $\langle a^k, a^\ell \rangle = \langle a^{NSD(k,\ell)} \rangle$

(3) $\langle a^k \rangle = \langle a^{NSD(k,n)} \rangle$ pro $n < \infty$

(4) $n < \infty \Rightarrow \left[G = \langle a^k \rangle \Leftrightarrow NSD(k,n) = 1 \right]$

(5) $n < \infty \Rightarrow$ G obsahuje právě $\varphi(d)$ prvků řádu d pro každé $d \mid n$

Důsledek: $\forall n \in \mathbb{N}$ platí $\boxed{\sum_{d \mid n} \varphi(d) = n}$.

Lemma: G konečná grupa
$\forall k$ se v G vyskytuje $\leq k$ prvků a splňujících $a^k = 1$ $\Rightarrow$ G je cyklická

Věta: Buď T těleso a $G \leq T^*$ konečná podgrupa. Pak G je cyklická.

Př.: Grupy $\mathbb{Z}_p^*$, p prvočíslo, jsou cyklické.

generátory $\mathbb{Z}_p^*$ = prvky řádu $p-1$ = PRIMITIVNÍ PRVKY
(jejich $\varphi(p-1)$)

DISKRÉTNÍ EXPONENCIÁLA $\quad exp_a : \mathbb{Z}_n \to G = \langle a \rangle$, $k \mapsto a^k$

DISKRÉTNÍ LOGARITMUS $\quad \log_a : G \to \mathbb{Z}_n$, $b \mapsto$ to jediné k t.ž. $b = a^k$

ELGAMALův protokol na šifrování s veřejným klíčem:

SETUP: zvol $G=\langle a\rangle$ $(n=|G|)$, $k\in\{2,\dots,n-1\}$ náhodně, $\boxed{b:=a^k}$

VEŘEJNÝ KLÍČ: G, a, b

TAJNÝ KLÍČ: k

ZAŠIFROVÁNÍ: zvol náhodně $r\in\{2..n-1\}$

$$x\in G \longmapsto (a^r,\ x\cdot b^r)\in G\times G$$

DEŠIFROVÁNÍ: $(u,v)\mapsto v\cdot u^{-k}$

SCHNORRův protokol na digitální podpis:

SETUP: zvol $G=\langle a\rangle \leq \mathbb{Z}_p^*$ t.ž. $|G|=q$ prvočíslo, $k\in\{2..q-1\}$ náhod., $\boxed{b:=a^k}$

VEŘEJNÝ KLÍČ: p, q, a, b

TAJNÝ KLÍČ: k

HASHOVACÍ FUNKCE: $H:\mathcal{M}\to\mathbb{Z}_q$

PODPIS: zvol náhodně $r\in\{2..q-1\}$

$$x\in\mathcal{M}\mapsto h:=H(a^r x)\in\mathbb{Z}_q\mapsto (r-k\cdot h,\ h)\in\mathbb{Z}_q\times\mathbb{Z}_q$$

OVĚŘENÍ: spočti $H(a^u b^h x)$, vyšlo h?

(dáno (u,h), zpráva x)