Grupa G se nazývá CYKLICKÁ pokud $G = \langle a \rangle_G$ pro nějaký prvek $a \in G$.

tj. $G = \{a^k : k \in \mathbb{Z}\}$, $G \simeq \mathbb{Z}$ / $\mathbb{Z}_n$

Tvrzení:

1. Podgrupy cyklických grup jsou cyklické.
2. $G = \langle a \rangle \Rightarrow \langle a^k, a^l \rangle = \langle a^{NSD(k,l)} \rangle$

   $G = \langle a \rangle, |G| = n \Rightarrow \langle a^k \rangle = \langle a^{NSD(k,n)} \rangle$
3. $G = \langle a \rangle \Rightarrow$
   - je-li G nekonečná, generátory jsou pouze a, a^{-1}
   - je-li $|G| = n$, generátory jsou právě prvky a^k : $NSD(k,n) = 1$
4. $G = \langle a \rangle, |G| = n \Rightarrow$ G obsahuje právě $\varphi(d)$ prvků řádu $d \mid n$

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

Lemma: Buď G konečná grupa, předpokládejme, že $\forall k$ obsahuje $\leq k$ prvků splňujících $a^k = 1$.
Pak G je cyklická.

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

Speciálně, multiplikativní grupy KONEČNÝCH TĚLES jsou CYKLICKÉ.

Tj. $\forall p \; \exists a$ t.ž. $\mathbb{Z}_p^* = \{a^0, a^1, \dots, a^{p-2}\}$

$\forall p, k, m \; \exists u$ t.ž. $\left(\mathbb{Z}_p[\alpha]/(m)\right)^* = \{u^0, \dots, u^{p^k-2}\}$

↳ není to určitě α
může být $\operatorname{ord}(\alpha) < p^k - 1$

Uvažujme cyklickou grupu $G = \langle a \rangle$ řádu n.

$\mathbb{Z}_n \longrightarrow G$

$k \longmapsto a^k$

jediné k t.ž. $a^k = b$ $\longleftarrow\!\shortmid$ b

!! $\log_a b$

... DISKRÉTNÍ EXPONENCIÁLA
... DISKRÉTNÍ LOGARITMUS
} v grupě G

Starší Tvrzení: Jsou to izomorfismy.

Empirický fakt: na výpočet EXP se často zná efektivní algoritmus $\sim \text{poly}(\log|G|)$

na výpočet LOG se v mnoha grupách nezná nic lepšího než brute force $\sim |G|$

↳ Př.: $\mathbb{Z}_p^*$, eliptické křivky

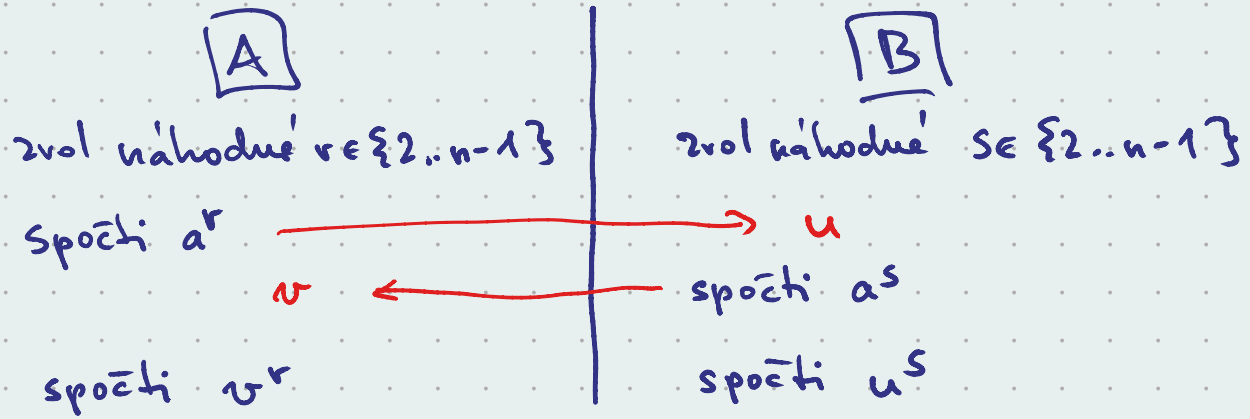
Bitcoin: digitální podpis Schnorrovým algoritmem

- křivka $y^2 - (x^3 + 7)$
- nad tělesem $\mathbb{Z}_p$ pro $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$
- $G := \langle A \rangle$ pro jistý bod A řádu $\approx 2^{257}$

DIFFIE-HELLMANův protokol na VÝMĚNU KLÍČE

přes otevřený kanál se dohodnout na společném tajném heslu

Uvažujme grupu $G = \langle a \rangle$ řádu n.



$$v^r = (a^s)^r = a^{rs} = (a^r)^s = u^s$$

↳ oba mají stejné heslo

SCHNORRův protokol na DIGITÁLNÍ PODPIS

Uvažujme grupu $G = \langle a \rangle$ řádu n.

Podepisující zvolí náhodně $k \in \{2 .. n-1\}$

spočte $\boxed{b = a^k}$

soukromý klíč : k

veřejný klíč : G, a, b a hashovací funkce $H: M \to \mathbb{Z}_n$

Podpis zprávy $x \in M$: zvol náhodně $r \in \{2 .. n-1\}$

spočti a^r

spočti $H(x, a^r)$

$\rightsquigarrow$ podpis $(r - k \cdot h, h) \in \mathbb{Z}_n \times \mathbb{Z}_n$

Ověření podpisu $(u, h) \in \mathbb{Z}_n \times \mathbb{Z}_n$:

spočti $g = a^u \cdot b^h$ v G

spočti $H(x, g)$

$\rightsquigarrow$ vyšlo h ?

$\Leftarrow$ $a^u \cdot b^h = a^{r-kh} \cdot b^h$

$= a^r \cdot (a^k)^{-h} \cdot b^h = a^r$