

(Diskret matte D, ht13: F20, ti 5 nov 2013)

## Cykliska grupper

$G$  är en **cyklisk grupp** om för något  $x \in G$  varje  $g \in G$  är  $x^n$  för något  $n \in \mathbb{Z}$ .

$x$  **genererar**  $G$ ,  $G = \langle x \rangle$ ,

$o(x) = m$  :  $C_m = \{1, x, x^2, \dots, x^{m-1}\} \approx (\mathbb{Z}_m, +)$

$o(x) = \infty$  :  $C_\infty = \{\dots, x^{-2}, x^{-1}, 1, x, x^2, \dots\} \approx (\mathbb{Z}, +)$

## Direkt produkt av grupper

Om  $A, B$  är grupper, är  $(A \times B, *)$  med  $(a_1, b_1) * (a_2, b_2) = (a_1 a_2, b_1 b_2)$  också en grupp, den **direkta produkten** av  $A$  och  $B$ .

Enligt kinesiska restsatsen gäller om  $\text{sgd}(m_i, m_j) = 1$  då  $i \neq j$  :

$$C_{m_1 \dots m_k} \approx C_{m_1} \times \dots \times C_{m_k}$$

## Delgrupper

$H$  är en **delgrupp** till  $(G, *)$  om  $H \subseteq G$  och  $(H, *)$  är en grupp.

**Sats:** Om  $G$  är en grupp och  $H \subseteq G$  gäller att

$$H \text{ är en delgrupp till } G \Leftrightarrow \begin{cases} S0 & H \neq \emptyset \\ S1 & x, y \in H \Rightarrow xy \in H \\ S2 & x \in H \Rightarrow x^{-1} \in H \end{cases}$$

Om  $H$  är **ändlig**, räcker  $S0$  och  $S1$ .