## Algoritmo di Shanks - esempio

- $G = \mathbb{Z}_{29}^*$ con generatore 2, $m = \lceil \sqrt{28} \rceil = 6$
- $2^{0 \cdot 6} = 1$, $2^{1 \cdot 6} = 6$, $2^{2 \cdot 6} = 7$, $2^{3 \cdot 6} = 13$, $2^{4 \cdot 6} = 20$, $2^{5 \cdot 6} = 4$
- $L_1 = \{(0, 1), (5, 4), (1, 6), (2, 7), (3, 13), (4, 20)\}$
- ora $2^{-1} = 15$; se $y = 17$,
- $17 \cdot 2^0 = 17$, $17 \cdot 2^{-1} = 15 \cdot 17 = 23$, $17 \cdot 2^{-2} = 26$, $17 \cdot 2^{-3} = 13$, $17 \cdot 2^{-4} = 21$, $17 \cdot 2^{-5} = 25$
- $L_2 = \{(3, 13), (0, 17), (4, 21), (1, 23), (5, 25), (2, 26)\}$

## Algoritmo di Shanks - esempio

- $G = \mathbb{Z}_{29}^*$ con generatore 2, $m = \lceil \sqrt{28} \rceil = 6$
- $2^{0 \cdot 6} = 1$, $2^{1 \cdot 6} = 6$, $2^{2 \cdot 6} = 7$, $2^{3 \cdot 6} = 12$, $2^{4 \cdot 6} = 20$, $2^{5 \cdot 6} = 4$
- $L_1 = \{(0, 1), (5, 4), (1, 6), (2, 7), (3, 13), (4, 20)\}$
- ora $2^{-1} = 15$; se $y = 17$,
- $17 \cdot 2^0 = 17$, $17 \cdot 2^{-1} = 15 \cdot 17 = 23$, $17 \cdot 2^{-2} = 26$, $17 \cdot 2^{-3} = 13$, $17 \cdot 2^{-4} = 21$, $17 \cdot 2^{-4} = 25$, $17 \cdot 2^{-5} = 25$
- $L_2 = \{(3, 13), (0, 17), (4, 21), (1, 23), (5, 25), (2, 26)\}$
- $x = m \cdot 3 + 3 = 18 + 3 = 21$

# Algoritmo di Shanks - esempio

- $G = \mathbb{Z}_{29}^*$ con generatore 2, $m = \lceil \sqrt{28} \rceil = 6$
- $L_1 = \{(0,1), (5,4), (1,6), (2,7), (3,13), (4,20)\}$
- possiamo riutilizzare $L_1$ anche per calcolare il LD per es di $y = 11$
- $11 \cdot 2^0 = 11, 11 \cdot 2^{-1} = 11 \cdot 15 = 20$
- qui $x = m \cdot 4 + 1 = 25$