

① We want to find  $(\alpha, \beta) \in \mathbb{N}^2$  s.t.  $g^{x+\alpha} \cdot h^{-(y+\beta)} = g^x \cdot h^{-y} \pmod{p}$ .

Let's denote by  $\alpha'$  and  $\beta'$  the order of  $g$  and  $h$  in  $\mathbb{Z}_p^*$ , respectively. It means

that  $g^{\alpha'} = 1 \pmod{p}$  and  $h^{\beta'} = 1 \pmod{p}$ . We have, for any  $(x, y) \in \mathbb{N}^2$ ,

$$g^{(\alpha'+x)} \cdot h^{-(y+\beta')} = g^{\alpha'} \cdot g^x \cdot h^{-y} \cdot h^{-\beta'} = (g^{\alpha'} \cdot h^{-\beta'}) \cdot g^x \cdot h^{-y} = (h^{\beta'})^{-1} \cdot g^x \cdot h^{-y} \stackrel{g^{\alpha'}=1 \pmod{p}}{=} (1)^{-1} \cdot g^x \cdot h^{-y} \stackrel{h^{\beta'}=1 \pmod{p}}{=} g^x \cdot h^{-y} \pmod{p}.$$

So, the fact. is periodic with period  $(\alpha', \beta')$ .

Given a period  $(\alpha, \beta)$ , you can compute the discrete logarithm. We know that

$$g^{x+\alpha} \cdot h^{-(y+\beta)} = g^x \cdot h^{-y} \pmod{p}. \text{ And this happens } \Leftrightarrow g^x \cdot h^{-\beta} = 1 \pmod{p}$$

$$\Leftrightarrow g^x = h^\beta \pmod{p}$$

$$\Leftrightarrow g^x = g^{\alpha \beta} \pmod{p}$$

$$\Leftrightarrow x = \alpha \cdot \beta^{-1} \pmod{q} \text{ where } q \text{ is the order of } g.$$