# Problem sheet 12 for Course 01410, 2025

## Exercise 1. (Period finding for breaking Diffie Hellman)

Recall the discrete logarithm problem: given $p \in \mathbb{N}$ and $g, h \in \mathbb{Z}_p^*$, find $a \in \mathbb{N}$ such that $g^a = h \bmod p$. It turns out that the discrete logarithm problem can also be solved via period finding. In this case, however, a two-dimensional version of period finding is needed. This 2D period finding problem is as follows: For a function $f : \mathbb{N}^2 \to \mathbb{N}$, find $\alpha, \beta \in \mathbb{N}$ such that $f(x + \alpha, y + \beta) = f(x, y)$ for all $x, y \in \mathbb{N}$. For the discrete logarithm problem as defined above, define

$$f(x, y) = g^x h^{-y} \bmod p.$$

Show that the function is periodic. Given a period $(\alpha, \beta)$, how can you compute the discrete logarithm?

## Exercise 2. (When will we have a cryptographically relevant quantum computer?)

Take a look at the 2024 Quantum Threat Timeline Report from the Global Risk Institute, available here:
`https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/`
When do we need to expect RSA and Diffie-Hellman as we use it today to be broken? What are the implications, when do you think do we need to switch to using post-quantum cryptography?