Exercise sheet 1, 10 February 2022

1. Watch the videos in the session for today, 11 Feb 2021.
   (I will not list this as an exercise on future sheets.)

2. Compute the order of $a = 7$ modulo $n = 15$ and use Shor's algorithm to factor n.

3. Compute the order of $a = 1124906$ modulo $n = 66887371$ and use Shor's algorithm to factor n.

4. Shor's algorithm also works to break discrete logarithms.
   Given g and $h \in \langle g \rangle$ find a function in g and h so that its period solves the discrete-logarithm problem $k = \log_g(h)$.
   Hint: Consider functions in two variables.
   "Period" here does not mean a unique or smallest repeat frequency, just some (s_1, s_2) with $f(x, y) = f(x + s_1, y + s_2)$.

   Spoiler alert: The next exercise has a big hint.

5. Show how finding a period of

   $$f_{g,h} : (x, y) \mapsto g^x h^y$$

   can be used to compute the discrete logarithm of h to base g.
   Note that the computations take place in some group $\langle g \rangle$ and you can assume that g has prime order.