1. Let $p = 11$
   (a) What are the possible orders for elements in $\mathbb{Z}_p^*$?
   (b) Find a generator a of $\mathbb{Z}_p^*$.
   (c) Fill in the following table:

k	$a^k \mod p$	$\text{ord}(a^k)$
1		
2		
$\vdots$		
p-1		

   (d) For which values of k is a^k a generator?
   (e) How are the values in your last answer related to $\phi(p-1)$?
   (f) How many generators does $\mathbb{Z}_p^*$ have?
   (g) What is a desirable *order* of α for DHKE using modulus p?
   What is a desirable *value* of α for DHKE using modulus p?

2. Repeat the previous problem with $p = 23$.
   Note that your table will have 22 rows.
   The Mathematica command MultiplicativeOrder[ ] might be handy.

3. Show that $p = 1\,786\,511$ is a poor choice as the modulus for DHKE.
   The Mathematica commands PrimeQ[ ] and FactorInteger[ ] may be useful.

4. Show that $p = 1\,786\,553$ is a reasonable choice for DHKE and find an appropriate value α.

5. Go to `https://www.rfc-editor.org/rfc/rfc3526` and verify that the given values for the 2048-bit prime and α are reasonable choices for DHKE.

   Note that when this page says “The generator is: 2”, it does *not* mean that 2 is a generator of $\mathbb{Z}_p^*$, but rather that $\alpha = 2$ is a good choice for Diffie-Hellman.