a) $Let p = 31. Find\ q(biggest\ prime\ dividing\ p)$.
b) $Which\ order\ h = 10\ base\ in\ \mathbb{Z}_{31}^*$.
c) $Knowing\ H\ and\ its\ order, find\ an\ element\ g = h^a\ of\ order\ 5$.
d) You have p = 13 (modulus prime) and q = 4. Find element of g.

Example, when I know *p* and *q*. (*result ???*)

Find an element g of order q_1 in $\mathbb{Z}_{p_1}$ Show computations.

Proof. **SOLUTION for $p_1 = 23$, $q_1 = 11$.**
Possible orders of elements are all the divisors of $\phi(23) = 22$, i.e. $1, 2, 11, 22$. I do not want a generator, I want an element a of order 11, i.e.,

Example, when I know *p* and *q*. (*result 7*)

Proof. **SOLUTION for $p = 29$ and $q = 7$.**
If $p = 29$ and $q = 7$, then g has order 7 in $\mathbb{Z}_{29}$
In this case $\phi(29) = 28 = 2^2 * 7$, the possible orders are $1, 2, 4, 7, 14, 28$.
Therefore, we have to find a element a, such that

$$\begin{cases} a^2 \not\equiv 1 & \mod 29 \\ a^4 \not\equiv 1 & \mod 29 \\ a^7 \equiv 1 & \mod 29 \end{cases}$$

We can try with $a = 2$:

$$\begin{cases} 2^2 = 4 \not\equiv 1 & \mod 29 \\ 2^4 = 16 \not\equiv 1 & \mod 29 \\ 2^7 = 2^5 * 2^2 \equiv 3 * 4 = 12 \not\equiv 1 & \mod 29 \end{cases}$$

2 has not order 7, but which one is the order of 2?
(FAST way to do the computation):
I continuous with the exponentiations of $a = 2$.

$$\begin{cases} 2^{14} \equiv (2 * 7)^2 \equiv 12^2 = 144 = 28 \equiv -1 \not\equiv 1 & \mod 29 \\ 2^{28} \equiv (-1)^2 \equiv 1 & \mod 29 \end{cases}$$

2 is a generator and has order 28. We use the fact that 7/28. Therefore,

$$(2^4)^7 \equiv 1$$

$$(16)^7 \equiv 1$$

In order to be sure that 16 has order 7, we must check that it does not have order 2 or 4.

$$\begin{cases} 16^2 = 256 \equiv 24 \not\equiv 1 & \mod 29 \\ 16^4 \equiv (-5)^2 = 25 \not\equiv 1 & \mod 29 \end{cases}$$

Now we can apply the algorithm:

Example, when I know *p* and *g*. (*result 8*)

Apply Diffie-Hellman algorithm where $p = p_1$, $g = g_1$ and q is the order of g.

Proof. **SOLUTION for $p_1 = 17$, $g_1 = 2$.**
We found that the order of $o(g_1) = 8$

Exercise when I know just p = 61. You find g and q (must be prime in this case).