Problems

1. **[2 pt]** Consider polynomials in $\mathbb{Z}_3[x]$
   (a) **[0.5 pt]** Show that $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$.
   (b) **[0.5 pt]** Find the number of elements in $\mathbb{Z}_3[x]_{x^2+1}$.
   (c) **[0.5 pt]** How many elements are there in $\mathbb{Z}_3[x]_{x^2+1}$?
   (d) **[0.5 pt]** Find a generator for $\mathbb{Z}_3[x]_{x^2+1}$, and verify your argument (i.e., check it is indeed a generator).

2. **[4 pt]** Suppose that we take the prime number $p = 41$ and $g = 6$.

   (a) **[1 pt]** Alice and Bob would like to share a random information(for example a random one-time key), which is a number between 1 to 40.

   - Alice has chosen the number 21 as her private key.
   - Bob has chosen the number 37 as his private key.

   What should Alice and Bob receive from each other as the public key, given the Diffie-Hellman key exchange method?

   (b) **[0.5 pt]** What is the information they shared (indicate the exact integer number)?

   (c) **[1 pt]** Now suppose that Alice and Bob has shared another random information (probably they have changed the private key and hence the public key generated from there as well). Charlie noticed that the public key of Alice is 15 and the the public key of Bob is 33. Charlie has followed MAT302 recently so he tried the following two ways to break the DHP via breaking the DLP, by using

   - **[1 pt]** The Brute force method
   - **[1 pt]** The Shanks' Babystep-Giantstep method

3. **[2 pt]** Recall we have explained the Elgamal method. Suppose that we still take the prime number $p = 41$ and $g = 6$.

   (a) **[1 pt]** Use the Oracle argument, show that the DHP is as secure as the Elgamal (We have proved one direction in lecture, you just need to prove the other direction.)

   (b) **[1 pt]**Now Suppose Alice has taken 14 as her private key. On the other hand Bob uses 31 as his one-time private key. He wants to share the number 29 with Alice. What should be the pair (c_1, c_2) that he sends to Alice?