IV054 Coding, Cryptography and Cryptographic Protocols
2013 - Exercises XI.

1. Consider `Bit commitment scheme` presented on the slide 13 in the Lecture 10.
   How can Bob be certain that Alice is using an $m \in QNR(n)$?

   Propose a way for Bob to verify this condition using only public information or show that it is not feasible (either by proving that yourself or by a reference to literature). How the protocol should work to disallow Alice's cheating while still being a bit commitment scheme.

2. Consider geometric constructions with a ruler (without markings) and a compass are allowed. We say a geometric object B is constructible from an object A if one can construct B starting with A using a finite numbers of the following operations:

   1. Given two distinct points, construct the line through both of them.
   2. Given two distinct points, construct the circle through one of them with center at the other.
   3. Given (two lines)/(two circles)/(a line and a circle) construct the (point(s) of) intersection.

   Eg. an angle is a geometric object consisting of two rays with a common end point. A well-known result from abstract algebra states that the trisection of an arbitrary angle is not constructible in the above sense.

   (a) Peggy claims that she knows the trisection of a publicly known angle $\beta = 3\alpha$. Construct an interactive protocol which allows to prove her claim. You may assume that Peggy can generate a random point on a circle and that Vic can flip a coin (uniformly at random).

   (b) Prove completeness and soundness of your protocol.

   (c) Prove that your protocol is zero-knowledge.

3. Here is useful link to the following interesting picture.

4. Three owners of a gold mine, Alfred, Brian and Christopher, are passionate poker players and they have access to an unlimited number of standard 52-card decks. They grew tired of splitting the income by 3 and each one has decided which one he would like to see dead. Because they all know this, they do not leave each other, so a face to face talk is not possible.

More on next page >>>

They want to figure out whether two of them agree on the man to kill. However, if A wants to kill B, he does not want to let B know that, unless B also wants to kill A or unless there is an agreement on whom to kill (if you tell somebody you want him killed, he might change his mind to kill you instead). They also do not want to allow anyone to cheat the process and they do not want to allow anyone to base his decision on any info they may get during the process. Of course, they will not vote themselves to be killed.

How they can figure out whether there is an agreement?

5.