# Assignment 3

### *Dark Forest*

***In DarkForest the move circuit allows a player to hop from one planet to another.***

***Consider a hypothetical extension of DarkForest with an additional ‘energy’ parameter. If the energy of a player is 10, then the player can only hop to a planet at most 10 units away. The energy will be regenerated when a new planet is reached.***

***Consider a hypothetical move called the ‘triangle jump’, a player hops from planet A to B then to C and returns to A all in one move, such that A, B, and C lie on a triangle.***

1. ***Write a Circom circuit that verifies this move. The coordinates of A, B, and C are private inputs. You may need to use basic geometry to ascertain that the move lies on a triangle. Also, verify that the move distances (A → B and B → C) are within the energy bounds.***

**[Answer]** <https://github.com/geesimon/zku/blob/main/week3/circuits/trianglejump.circom>

<https://github.com/geesimon/zku/blob/main/week3/circuits/rangecheck.circom>

1. *[****Bonus****]* ***Make a Solidity contract and a verifier that accepts a snark proof and updates the location state of players stored in the contract.***

**[Answer]**

<https://github.com/geesimon/zku/blob/main/week3/contracts/trianglejump.sol>

***文本

描述已自动生成***

### *Fairness in card games*

### *MACI and VDF*

### *InterRep*

### *Thinking in ZK*

1. ***If you have a chance to meet with the people who built DarkForest and InterRep, what questions would you ask them about their protocols?***