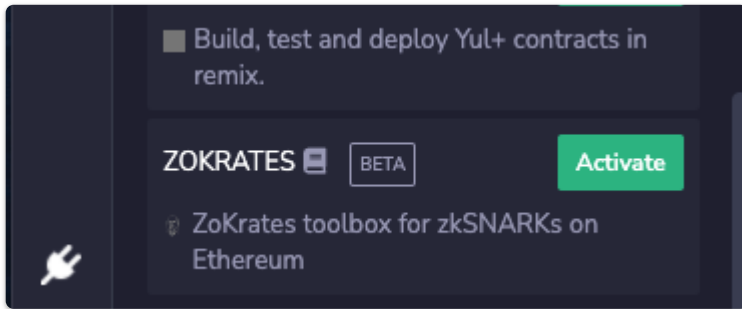


Homework 3

Practice using Zokrates

Use [Remix](#)

Install the Zokrates plugin



1. Use the example file to generate a proof to show that a prover knows the square root of 25.
2. Try to create an invalid proof [Manually edit the proof, but verifier should reject it](#)
3. Follow the example to build a proof that you know the pre image of a hash
<https://zokrates.github.io/examples/sha256example.html>
4. In principle how could you use Zokrates to verify that a certain address on Ethereum has more than say 1 ETH ?

[We can use public inputs from contracts and use that in the verifier contract, however source has to be trusted](#)