

Homework 5

Implement a solidity contract that verifies the computation for the EC points.

$$0 = -A_1B_2 + \alpha_1\beta_2 + X_1\gamma_2 + C_1\delta_2$$

$$X_1 = x_1G_1 + x_2G_1 + x_3G_1$$

Pick any (nontrivial) values to generate the points that results a balanced equation.

Note that x_1, x_2, x_3 are uint256 and the rest are G_1 or G_2 points.

You will need to take in the following as arguments to a public function:

$$A_1, B_2, C_1, x_1, x_2, x_3$$

Use the ethereum precompiles for addition and multiplication to compute X , then the precompile for pairing to compute the entire equation in one go.

All other points should be hardcoded into the contract. For example, suppose you want

$$\alpha_1 = 5G_1$$

$$\beta_2 = 6G_2$$

...

You need to compute those values and write them as constants inside the contract.

Tip: make the pairing work with only two sets of points (2 G_1 and 2 G_2) first for simple examples. The order for G_2 in the precompile is not what you are expecting it to be!

