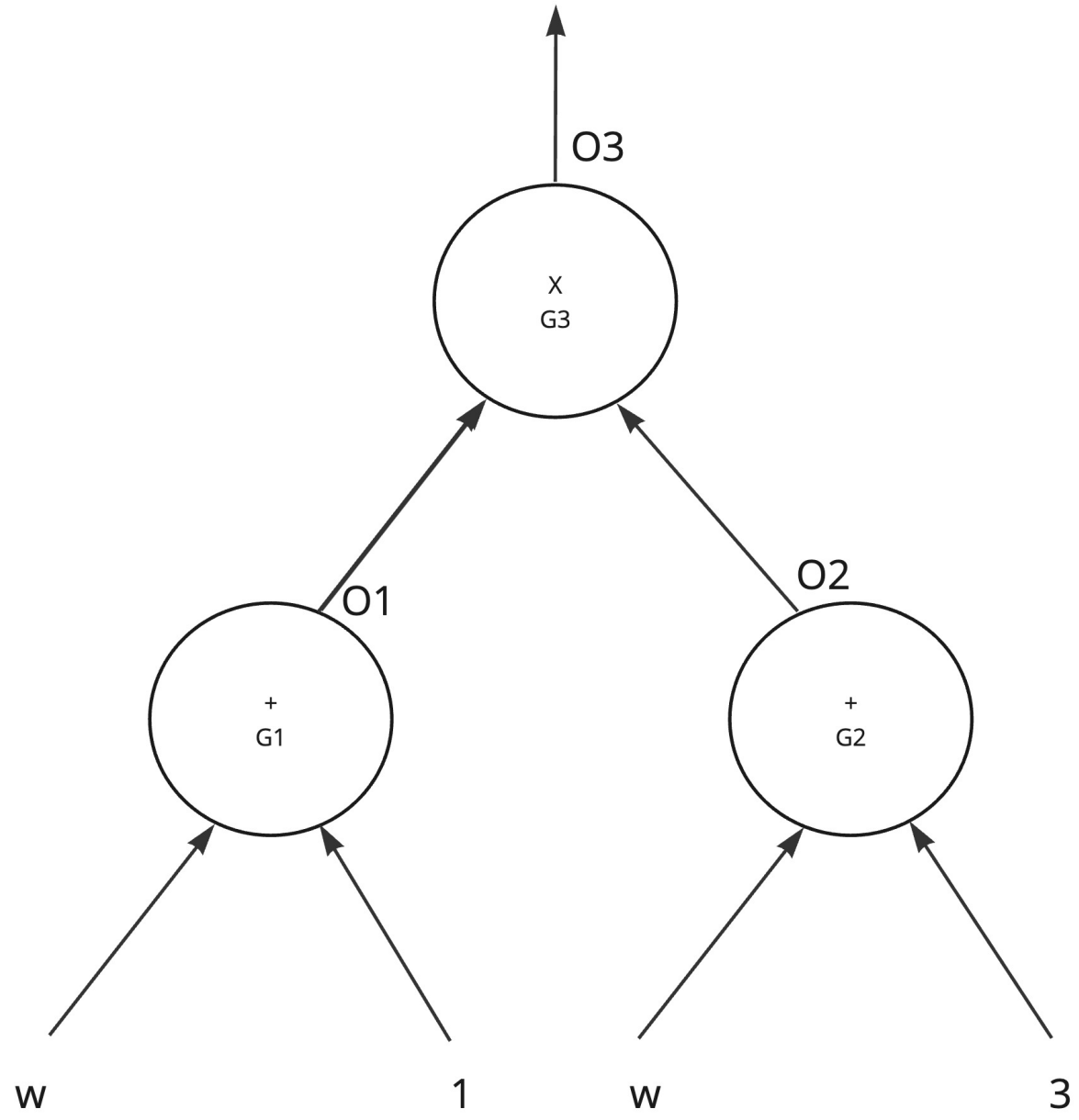
Homework 12

1. Watch these videos
   [ZK Proofs what are they good for]
   [Halo2 circuits]
   [Performance and Security]
2. Arithmetic circuits

> **Example arithmetic circuit**
>
> Taking this example, we have 3 gates :
>
> G1 an addition gate, with output O1
> G2 an addition gate with output O2
> G3 a multiplication gate with output O3



1. Thinking of the output O3, what polynomial does this represent (our variable is w)
2. If the output O3 is required to be 24, can you find a satisfying value of w
3. For each gate write out a constraint in terms of the inputs and outputs
4. Can you add selectors S1, S2, S3 for the constraints you have written

See page 3

1- $(w+1) * (w+3) = 03$

2- $w^2 + 4w + 3 = 24$

$w^2 + 4w - 21 = 0$

21 is divisible by

1 -1

3 -3

7 -7

	1	4	-21
3		3	21
	1	7	0

$x = 3$

3- G_1

$= w + 1 = 01$

G_2

$= w + 3 = 02$

$G_3 = G_1 \cdot G_2 = 03$

$= (w+1) \cdot (w+3) = 03$

4- G_1

$S_1(a_1 + b_1) - C_1 = 0$

$S_1(w+1) - 01 = 0$

G_2

$S_2(a_2 + b_2) - C_2 = 0$

$S_2(w+3) - 02 = 0$

G_3

$(1 - S_3) \cdot G_1 \cdot G_2 - 03 = 0$

$(1 - S_3) \cdot (S_1(a_1 + b_1) - C_1) \cdot (S_2(a_2 + b_2) - C_2) - C_3 = 0$