Euclid Algorithm

We know from the lecture that $\gcd(a, b) = \gcd(a, R_a(b))$.
This gives rise to the Euclid Algorithm:

```
Euclid(a, b):
    if a < b:
        swap(a,b)
    while b ≠ 0:
        a = R_b(a)
        swap(a, b)
    return a
```

In practice it looks like this. Say we want to find the gcd of 105 and 30:

① 105 30 We calculate $R_{30}(105) = 15$.

② 30 15 We calculate $R_{15}(30) = 0$

③ 15 0

④ $\gcd(105, 30) = 15$

So in words: We simply find the larger number and calculate the remainder of it and replace it with that. Then we repeat this until one number is 0. The other number is the gcd.

Another example: Calculate the gcd of 110 and 21:

① 110 21

② 21 5 since $110 = 21 \cdot 5 + 5$

③ 5 1 since $21 = 5 \cdot 4 + 1$

④ 1 0 since $5 = 1 \cdot 5 + 0$

So the gcd is 1.

Extended Euclid

Say we want to not only find $\gcd(a,b)$, but also find the numbers λ, μ such that $\lambda a + \mu b = \gcd(a,b)$.

This is for example useful if we need to find the multiplicative inverse of a modulo b.
Because if we find λ, μ with $\lambda a + \mu b = 1$ then we know that $\lambda a \equiv_b 1$ and so λ is the inverse of a modulo b.

For the extended euclid algo we do the same thing, but also keep track of the numbers λ and μ which give us the remainder. Here for 105 and 30:

Remainder	λ	μ	
105	1	0	since $1 \cdot 105 + 0 \cdot 30 = 105$
30	0	1	since $0 \cdot 105 + 1 \cdot 30 = 30$
15	1	-3	since $1 \cdot 105 - 3 \cdot 30 = 15$
0	-2	7	since $-2 \cdot 105 + 7 \cdot 30 = 0$

This looks confusing, so let's do a longer example so we see what is going on. Note that our two numbers will now always be the last two in the table and not be side by side.

Find λ, μ s.t. $\lambda 240 + \mu 46 = \gcd(240, 46)$.

	Remainder	λ	μ	
①	240	1	0	We start like this since $240 \cdot 1 = 240$ and $46 \cdot 1 = 46$.
②	46	0	1	

Now we find that $46 \cdot 5 + 10 = 240$ and so $R_{46}(240) = 10$.
So we can write 10 in the next entry. But we still need to find λ and μ. Well:

$240 = 46 \cdot 5 + 10$

$\Rightarrow 10 = 240 - 5 \cdot 46$ and so $\lambda = 1$ and $\mu = -5$

③	10	1	-5	

Okay, now we work with 46 and 10. We find that $10 \cdot 4 + 6 = 46$. So our next number is 6 and:

$10 \cdot 4 + 6 = 46$

$\Rightarrow 6 = 46 - 10 \cdot 4$ and since we know $10 = 1 \cdot 240 - 5 \cdot 46$

$\Rightarrow 6 = 46 - 4 \cdot (240 - 5 \cdot 46)$

$\Rightarrow 6 = -4 \cdot 240 + 21 \cdot 46$

④	6	-4	21	

But look at the equation again:

$$6 = \underset{\uparrow}{46} - 4 \cdot \underset{\uparrow}{10}$$

(2) (3)

We can simply read of the λ and μ from the rows above, so if we want to find them for row (4) we can do

$$1 \cdot (2) - 4 \cdot (3) = (0,1) - 4(1,-5)$$

$$= (0,1) + (-4, 20)$$

$$= (4, 21)$$

which is a lot easier. So for the next row:

We find $10 = 1 \cdot 6 + 4$ so the next number is 4 and for the rows we have

$$4 = 10 - 1 \cdot 6 \Rightarrow 1 \cdot (1,-5) - 1 \cdot (-4, 21) = (5, -26)$$

(5)	4	5	-26

And then since $R_4(6) = 2$ and $1 \cdot 6 - 1 \cdot 4 = 2$:

(6)	2	-9	47
(7)	0	23	-120

And so $-9 \cdot 240 + 47 \cdot 46 = 2 = gcd(240, 46)$

Don't worry if you didn't understand this on the first try. There are lots of videos and tutorials on the internet which explain it more in-depth!