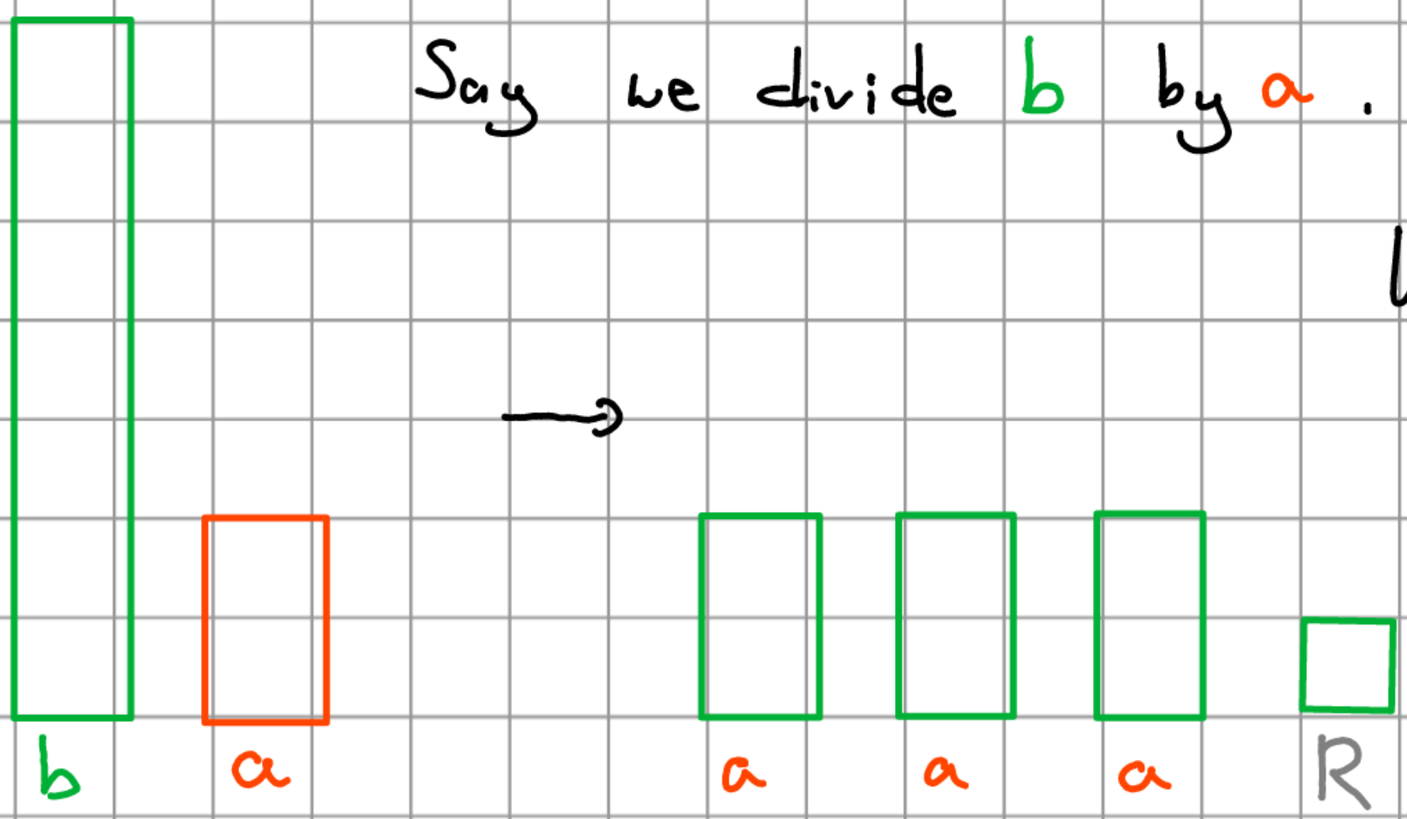
Number Theory - Intuition

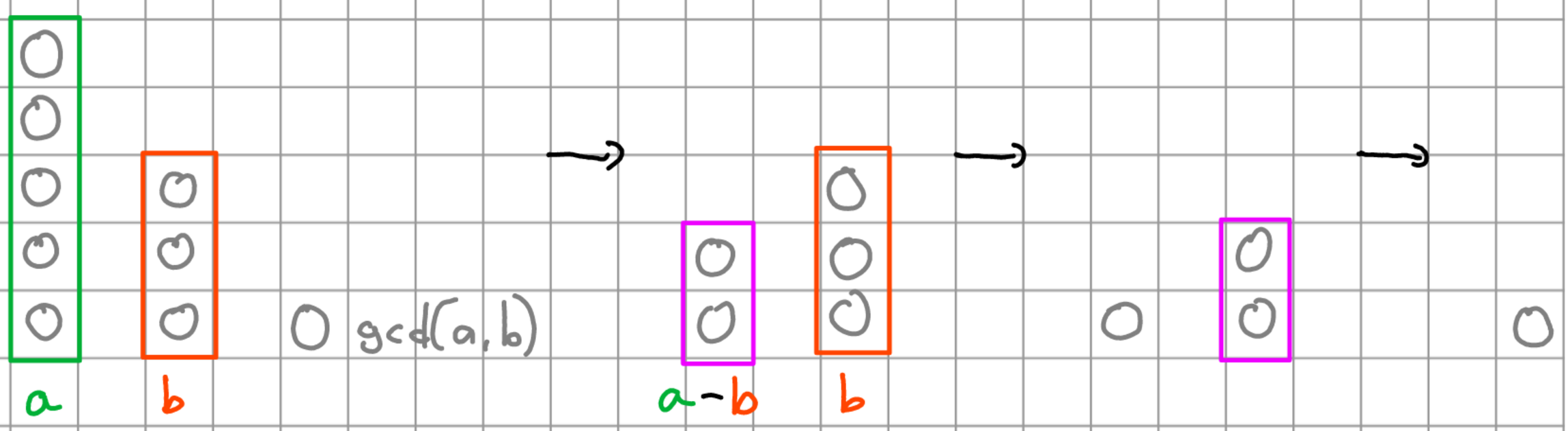
What is the remainder?

Say we divide b by a.



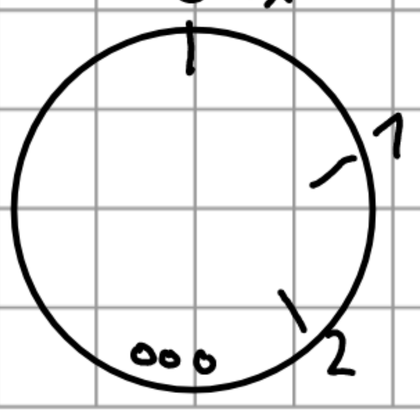
We get $b = 3a + R$

Why is $\gcd(a, b) = \gcd(a-b, b)$?

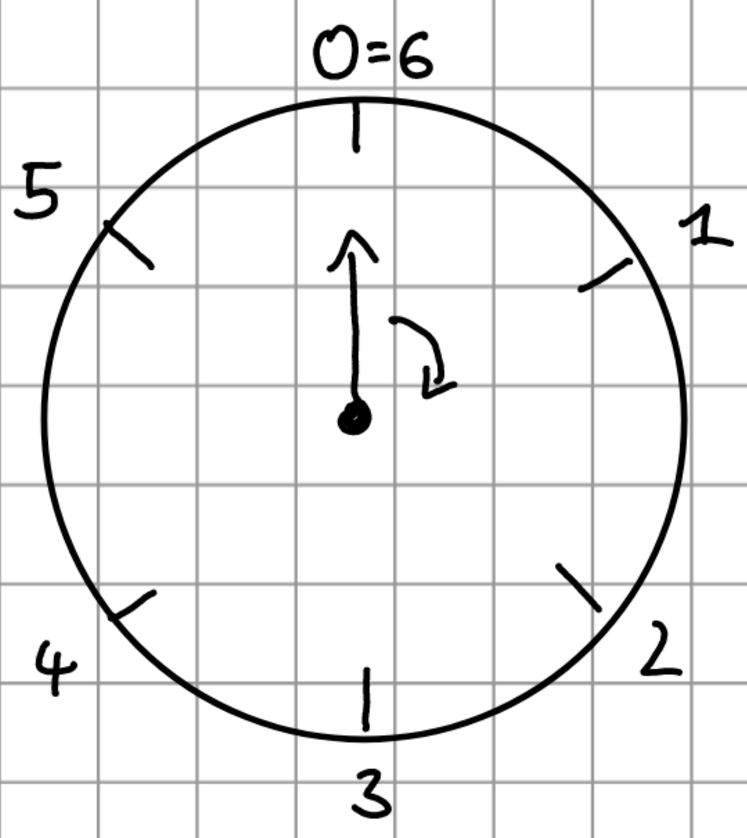


Modulos?

Imagine calculating in the space $\equiv_x$ as calculating on a clock instead of a number line:



So for modulo 6:

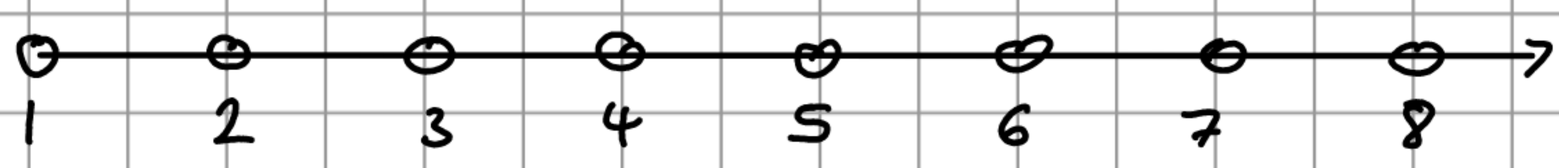


Now when we take $17 \equiv_6$ we simply rotate the arrow by 17 steps. Since every 6 steps we land on 0 again, we land at 5.

Adding $x + 3$ means moving the arrow by 3 steps.

Now for example $17 \cdot 3 + 4 \equiv_6$?
Well, we move the arrow 3 times by 17 steps, but since moving by 6 steps doesn't change anything, we move 3 times by 5 steps. So this is 15 steps, which is 3 steps. Now plus 4 steps is 7 is 1 step. So it is 1.

If we now "roll-out" the clock onto a number line we get:



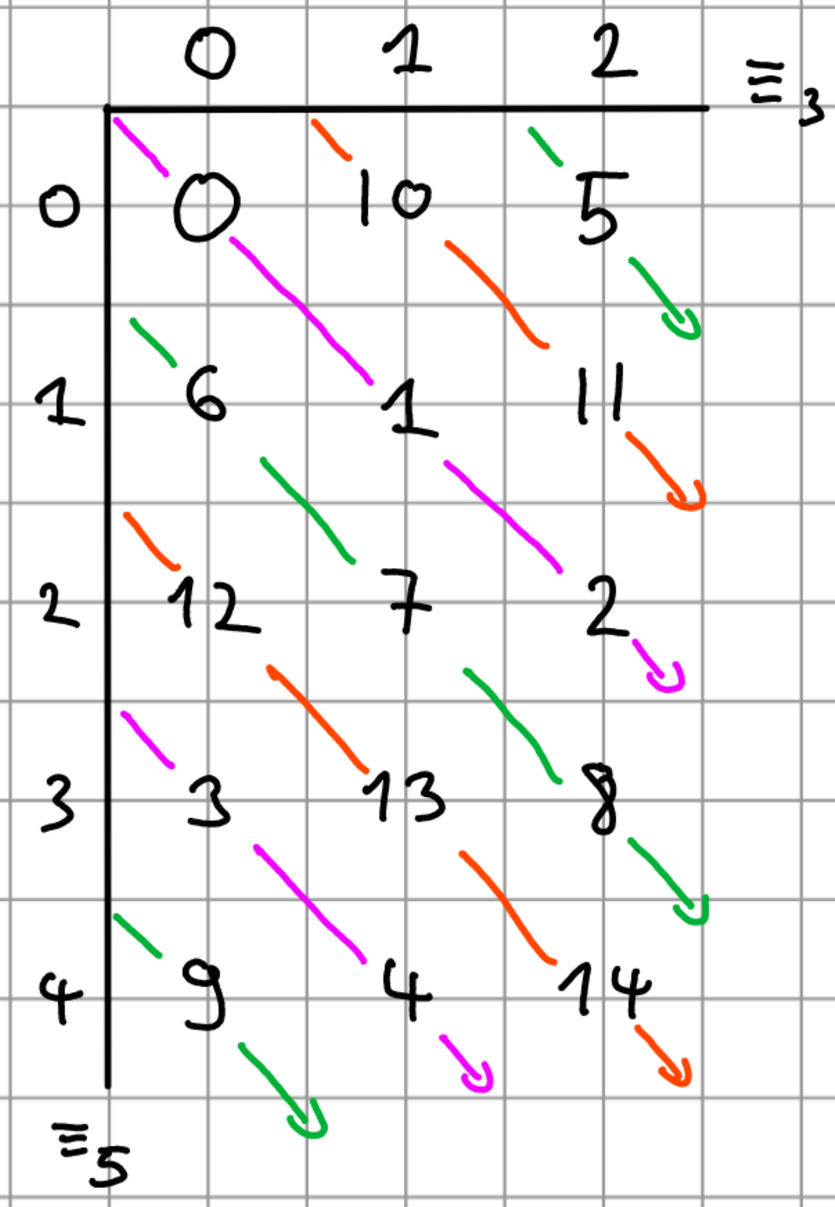
mod 2	1	0	1	0	1	0	1	0
mod 3	1	2	0	1	2	0	1	2
mod 5	1	2	3	4	0	1	2	3
mod 7	1	2	3	4	5	6	0	1

Chinese Remainder Theorem?

Say we have a system of equations like

$$x \equiv_3 a \quad \text{and} \quad x \equiv_5 b .$$

Now let us write down all possible combinations of a and b in a matrix:



You can see that the solutions are spiraling around the matrix like a candy cane!

And every solution is hit exactly once!

If we try the same thing with two numbers which are not coprime then we would fail. Try it for 2 and 4 for example!

If we extend this to more dimension, then it still works. (Imagine adding $x \equiv_2 c$ here. Then it would jump back and forth in the 2-dimension and spiral two times, since 15 hits 0 again, but now with $15 \equiv_2 1$ and not $0 \equiv_2 0$.)