Modulo-Equations
The Brute-Force Method

Say you have a system of equations like:

$$x \equiv_2 1$$
$$x \equiv_3 2$$
$$x \equiv_5 4$$

Now how do you find the solutions? You could of course use the CRT-Algorithm, but you can also use brute-force:

① Write down a number line:

0 1 2 3 4 5 6 7 8 9 10 11 12 ....

+1 +1 +1 +1 +1 ....

Step-width = 1

② Tackle the first equation:

How do we do that? Well, first we find the first number on the line which satisfies $x \equiv_2 1$. That is 1 here. Then we multiply the step-width by our modulo x from $\equiv_x$:

1 3 5 7 9 11 12 13 15 16 ....

+2 +2 +2 ....

Step-width = 2

③ For the second equation we do the same thing. The first number x which satisfies $x \equiv_3 2$ on our line is 5. So we start at 5 with our new step-width $= 2 \cdot 3 = 6$:

5 11 17 23 29 35 41 47 ...

$5 \xrightarrow{+6} 11 \xrightarrow{+6} 17 \xrightarrow{+6} 23$

Step-width $= 6$

④ Same thing again. The first number satisfying $x \equiv_5 4$ is 29 here. So we start at 29 with step-width $6 \cdot 5 = 30$:

29 59 89 119 ...

and all solutions are: $29 + k \cdot 30$ for $k \in \mathbb{N}$!

Why this works? We simply go through the equations one by one and only keep the numbers that satisfy it. Since all the numbers x in $\equiv_x$ are coprime we know that for step-width s and first solution A for $A \equiv_x b$, that the next solution is

$$A + s \cdot x$$

because $R_x(A + s \cdot x) = R_x(A) + R_x(sx) = b + 0 = b$.

But for any $y \neq x$ we get $R_x(A + sy) = R_x(A) + R_x(sy) = b + z$ for $z \neq 0$ since x and s are coprime.