Notes on the algorithm for the Chinese Remainder Theorem

1. In general $x \equiv a \bmod m$, $x \equiv b \bmod n$, $\gcd(m,n)=1$, so there exists r, s such that $rm+sn=1$.

$x \equiv a \bmod m \Rightarrow x = a+mt$ for some t to get

$x \equiv b \bmod n \Rightarrow a+mt \equiv b \bmod n \Rightarrow mt \equiv b-a \bmod n$.

Now $rm+sn=1$ so $rm = 1-sn \Rightarrow rm \equiv 1 \bmod n$!

$mt \equiv b-a \bmod n$ multiply by r

$r(mt) \equiv r(b-a) \bmod n \Rightarrow (rm)t \equiv r(b-a) \bmod n$.

Since $rm \equiv 1 \bmod n$, $1 \cdot t \equiv r(b-a) \bmod n$

and $t \equiv r(b-a) \bmod n \Rightarrow t = r(b-a)+nu$ for some u

$\Rightarrow x = a+mt = a+m(r(b-a)+nu) = a+rm(b-a)+mnu$

$\Rightarrow$ $x \equiv a+rm(b-a) \bmod mn$

Do not try to memorize the answer, memorize the method

2. $x \equiv 1 \bmod 3 \Rightarrow x = 1+3t$ (Class Example)

$x \equiv 3 \bmod 5$

$1+3t \equiv 3 \bmod 5 \Rightarrow 3t \equiv 3-1 \equiv 2 \bmod 5$.

Here, you need to find the multiplicative inverse of 3 mod 5

$2 \cdot 3 = 6 \equiv 1 \bmod 5$ (or, as usual, $3 \cdot 2 + 5(-1) = 1$)

So $3t \equiv 2 \bmod 5 \Rightarrow 2(3t) \equiv 2(2) \bmod 5$

$\Rightarrow 6t \equiv 4 \bmod 5$

$\Rightarrow t \equiv 4 \bmod 5$ (because $6 \equiv 1 \bmod 5$)

So $t = 4+5u$

$x = 1+3t$

$x = 1+3(4+5u) = 1+12+15u = 13+15u$

$x \equiv 13 \bmod 15$