Chinese Remainder by example

$x \in \mathbb{Z}_{15} \longrightarrow (x \bmod 3,\ x \bmod 5) \in \mathbb{Z}_3 \times \mathbb{Z}_5$

$x \in \mathbb{Z}_{15}$	$x \bmod 3$	$x \bmod 5$
0	(0 ,	0)
1	(1 ,	1)
2	(2 ,	2)
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

solve for

$$\begin{cases} x \equiv_3 1 \\ x \equiv_5 2 \end{cases}$$

get 7

$\mathbb{Z}_{18} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_6$

$\mathbb{Z}_{18}$	$\mathbb{Z}_3$	$\mathbb{Z}_6$
0	0	0
1	1	1
2	2	2
3	0	3
⋮		
?? $\longrightarrow$	1	2

things like (1, 2) never appear

no solution to

$$\begin{cases} x \equiv_3 1 \\ x \equiv_6 2 \end{cases}$$

$\mathbb{Z}_{18} \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_9$

$\mathbb{Z}_{18}$
0
1
2
3
⋮

this works

$4 + 9 \mod 15$

$= 13$

$\mathbb{Z}_{15}$ $\rightarrow$	$x \bmod 3$	$x \bmod 5$
0	(0 ,	0)
1	(1 ,	1)
2	(2 ,	2)
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

$\mathbb{Z}_3$ $\quad$ $\mathbb{Z}_5$

$(1, 4)$

$+ \; (0, 4)$

$$\begin{pmatrix} 0+1 \mod 3, \\ 4+4 \mod 5 \end{pmatrix}$$

$= (1, 3)$

$4 \times 9 \mod 15$

$= 6$

$\mathbb{Z}_{15}$ $\rightarrow$	$x \bmod 3$	$x \bmod 5$
0	(0 ,	0)
1	(1 ,	1)
2	(2 ,	2)
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

$(1, 4)$

$* \; (0, 4)$

$\downarrow$

$$\begin{pmatrix} 0 \cdot 1 \mod 3, \\ 4 \cdot 4 \mod 5 \end{pmatrix}$$

$= (0, 1)$

$\mathbb{Z}_{15}^*$

$\mathbb{Z}_{15}$	$\mathbb{Z}_3$: x mod 3	$\mathbb{Z}_5$: x mod 5	$\mathbb{Z}_3^*$	$\mathbb{Z}_5^*$
0	0	0	0	0
1	1	1	1	1
2	2	2	2	2
3	0	3	0	3
4	1	4	1	4
5	2	0	2	0
6	0	1	0	1
7	1	2	1	2
8	2	3	2	3
9	0	4	0	4
10	1	0	1	0
11	2	1	2	1
12	0	2	0	2
13	1	3	1	3
14	2	4	2	4

$$\begin{tikzcd}
\boxed{x} & & \boxed{(u,v)} \\
\mathbb{Z}_{rs} \arrow[rr, bend left, "(x \% r,\ x \% s)"] \arrow[d, "\begin{array}{l}\text{addition,}\\ \text{multiplication}\\ \text{mod } rs\end{array}"'] & & \mathbb{Z}_r \times \mathbb{Z}_s \arrow[ll, bend left, "\begin{array}{c}\text{chinese}(u,v)\\ \text{(only if } \gcd(r,s)=1)\end{array}"] \arrow[d, "\begin{array}{l}\text{addition,}\\ \text{multiplication}\\ \text{component-wise}\end{array}"] \\
\mathbb{Z}_{rs} \arrow[rr, bend left, "(x \% r,\ x \% s)"] & & \mathbb{Z}_r \times \mathbb{Z}_s \arrow[ll, bend left, "\begin{array}{c}\text{chinese}(u,v)\\ \text{(only if } \gcd(r,s)=1)\end{array}"]
\end{tikzcd}$$

In this picture, two green paths always give same answer

$x, y \in \mathbb{Z}_N$ $\qquad\qquad (N = p \cdot q)$

CRT way of computing $x + y \bmod N$

$$
\begin{array}{rcl}
x & \longrightarrow & (x \% p,\ x \% q) \\
+\ y & \longrightarrow & (y \% p,\ y \% q) \\
\hline
z & \xleftarrow[\text{chinese()}]{} & (x+y \% p,\ x+y \% q)
\end{array}
$$

CRT way of computing $xy \bmod N$

$$
\begin{array}{rcl}
x & \longrightarrow & (x \% p,\ x \% q) \\
*\ y & \longrightarrow & (y \% p,\ y \% q) \\
\hline
z & \xleftarrow[\text{chinese()}]{} & (xy \% p,\ xy \% q)
\end{array}
$$

CRT way of computing $c^d \bmod N$

$$
\begin{array}{rcl}
c & \longrightarrow & (c \% p,\ \ c \% q) \\
\text{exponentiate mod } N \downarrow & & \ \ \downarrow \qquad\qquad \downarrow \\
c^d & \xleftarrow[\text{chinese()}]{} & (c^d \% p,\ c^d \% q)
\end{array}
$$

RSA:

$N \quad p \quad q \quad \underline{e \quad d} \quad \varphi \quad m \quad c$

p, q primes (distinct)

$N = pq$

φ is Euler's totient function

$\varphi(N) = (p-1)(q-1)$

e, d exponents; $\quad ed \equiv_{\varphi(N)} \underline{1}$

RSA $\quad m \longrightarrow m^e \bmod N$

inverse $\quad c \longrightarrow c^d \bmod N$