Chinese Remainder Theorem:

What it says: we can solve a system of (modular) equations.

Why we want it: it gives us the inverse of the canonical injection:

$$n = p_1^{e_1} \cdots p_n^{e_n} \qquad \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{e_n}\mathbb{Z} \\ \bar{a} & \longmapsto & (\bar{a}, \dots, \bar{a}) \end{array}$$

By the Chinese Remainder Theorem, this has an inverse:

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longleftarrow & \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{e_n}\mathbb{Z} \\ \bar{x} & \longleftarrow & (\bar{c_1}, \dots, \bar{c_n}) \end{array} \qquad \text{with } (\bar{c_1}, \dots, \bar{c_n}) = (\bar{x}, \dots, \bar{x}).$$

Remark: p prime, then $\mathbb{Z}/p\mathbb{Z}$ has all elements invertible since they are all coprime with p. Moreover, the only non-invertible elements of $\mathbb{Z}/p^e\mathbb{Z}$, $e \in \mathbb{N}$

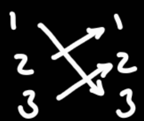
Result: $a \in \mathbb{Z}/m\mathbb{Z}$ is invertible iff $\gcd(a, m) = 1$.

are the elements of the form p^r with $r < e$, $r \in \mathbb{N}$.

Permutation:

A permutation is a bijection of sets.

Take $S = \{1, \dots, n\}$. A permutation of S is a function of sets $f : S \longrightarrow S$ that is bijective. Such a function assigns to a number $\begin{smallmatrix}1\\ \vdots \\ n\end{smallmatrix}$ a unique $\begin{smallmatrix}1\\ \vdots \\ n\end{smallmatrix}$.

Example: $S = \{1, 2, 3\}$, we have  so $f(1) = 3$, $f(2) = 1$, $f(3) = 2$

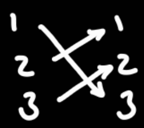
gives one permutation of S.

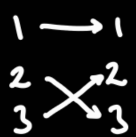
Matrix notation: $\begin{array}{l} \text{input} \\ \text{output} \end{array} \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}$.

Concatenation: $(1 \; f(1) \; f(f(1)) \cdots f^k(1) \; 1)(a \; f(a) \; f(f(a)) \cdots f^j(a) \; a) \cdots$

$a \neq f^i(1) \;\; \forall i$

this terminates because S is finite.

Example: The function  is: $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ as well as $(1 \; 3 \; 2)$.

Now:  is: $(1)(2\,3) = (2\,3)$.

To compose permutations we do one after the other:

$(1\,2\,3)(2\,3)(1\,3) = \begin{array}{l} 1 \rightarrow 3 \rightarrow 2 \rightarrow 3 \\ 2 \rightarrow 3 \rightarrow 1 \\ 3 \rightarrow 1 \rightarrow 2 \end{array} = (1\,3\,2)$