Chinese Reminder Theorem

$Definition: ---$

$Theorem:$

CRT state that you can recover any number from its residu modulo, in the following way
$for\ 1 \leqslant i, j \leqslant k\ \ and\ i \neq j\ with\ gcd(m_i, m_j) = 1,\ we\ declare\ M = \prod_{i=1}^{k} m_i,\ for\ which\ every\ m_i$
$is\ in\ \mathbb{Z}_{m_i},\ any\ number\ A\ inside\ \mathbb{Z}_M\ can\ be\ expressed\ as\ (a_1, ..., a_k)\ k-tuple\ value\ with$
$a_i = A \bmod m_i,\ and\ we\ can\ reconstruct\ A\ from\ thoes\ k-tuple\ and\ its\ a\ unique\ set\ of\ values,$
$we\ can\ say\ that\ there\ is\ some\ fuction\ \phi\ that\ is\ bijectif\ and\ verify$

$$\phi : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_k}$$
$$A \to \phi(A) = (a_1, ..., a_k)$$

and

$$\phi^{-1} : \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_k} \to \mathbb{Z}_M$$
$$(a_1, ..., a_k) \quad \to \phi^{-1}(a_1, ..., a_k) = A$$

$Proof:$

$for\ 1 \leqslant i, j \leqslant k\ \ and\ i \neq j\ with\ gcd(m_i, m_j) = 1,\ we\ declare\ M = \prod_{i=1}^{k} m_i,\ for\ which\ every$
$m_i \in \mathbb{Z}_{m_i},\ any\ number\ A\ inside\ \mathbb{Z}_M,\ we\ can\ easly\ construct\ the\ k-tuple\ values\ for\ any$
$1 \leqslant i \leqslant k\ with\ a_i = A \bmod m_i,\ for\ the\ other\ way\ we\ need\ to\ construct\ the\ number\ in\ way\ that$
$can\ reproduce\ the\ k-tuple\ for\ every\ m_i,\ that\ means\ \sum_{i=1}^{k} a_i c_i\ with\ c_i \bmod m_j = 0\ if\ i \neq j$
$and\ c_i \bmod m_j = 1\ if\ i = j,\ we\ can\ do\ that\ by\ introducing\ M_i = \frac{M}{m_i}\ which\ clearly\ give\ use\ that$
$gcd(M_i, m_i) = 1,\ mean\ that\ M_i\ has\ a\ inverse\ multiplicative\ with\ m_i,\ we\ can\ write\ c_j\ as$
$c_j = M_j \times \left(M_j^{-1} \bmod m_j\right),\ so\ that\ c_j \bmod m_j = \left(M_j \times \left(M_j^{-1} \bmod m_j\right)\right) \bmod m_j\ then\ we\ can$
$use\ modular\ arithmetics,\ to\ have\ c_j \bmod m_j = \left(M_j \times M_j^{-1}\right) \bmod m_j = 1 \bmod m_j,\ and\ we\ can$
$also\ observe\ that\ c_j\ is\ written\ as\ M_j \times q\ with\ q = M_j^{-1} \bmod m_j,\ so\ any\ i \neq j\ will\ equal\ to$
$0 \bmod m_i,\ hence\ if\ we\ add\ all\ the\ result\ from\ each\ a_i c_i\ and\ preforme\ \left(\sum_{i=1}^{k} a_i c_i\right) \bmod m_l\ we\ will$
$have\ exactly\ a_l,\ for\ safety\ we\ add \bmod M\ to\ the\ sum\ so\ that\ we\ are\ sure\ it\ stays\ in\ Z_M\ hence$
$A = \left(\sum_{i=1}^{k} a_i c_i\right) \bmod M,\ this\ is\ unique\ because\ suppose\ A, A' \in \mathbb{Z}_M,\ with\ each\ a\ has\ the\ same\ a_i$

$k-tuples,\ that\ means\ A \equiv A' \bmod m_i\ for\ each\ i,\ implying\ (A-A') = 0 \bmod m_i\ for\ each\ i$
$m_i|(A-A'),\ that\ mean\ M|(A-A')\ hence\ A \equiv A' \bmod M.$
