O TEOREMA CHINÊS DO RESTO

SEJAM $m_1, \dots, m_k$ T.Q. $m_i \perp m_j$ PARA TODO $i \neq j$ E TOME $m = m_1 \cdots m_k$
DADOS $x_1, \dots, x_k$, EXISTE UM ÚNICO NÚMERO $x \in \{0, \dots, m-1\}$ T.Q.

$$x \equiv x_i \pmod{m_i} \quad \text{PARA TODO } i$$

PROVA: PARA CADA i, TOME $M_i = \prod_{j \neq i} m_j$ E DEFINA a_i T.Q

$$M_i \cdot a_i \equiv 1 \pmod{m_i}$$

TOME $x = \sum_{i=1}^{k} x_i M_i \cdot a_i$.

NOTE QUE PARA TODO i, TEMOS

$$x \equiv x_i M_i a_i \pmod{m_i}$$

PORQUE SE $j \neq i$, ENTÃO M_j É MÚLTIPLO DE m_i, E PORTANTO TEMOS $x_j M_j a_j \equiv 0 \pmod{m_i}$.

FINALMENTE PELA DEFINIÇÃO DE a_i, TEMOS $x_i M_i a_i \equiv x \pmod{m_i}$

UNICIDADE: SUPONHA QUE x E y SEJAM DUAS SOLUÇÕES.
ENTÃO PARA TODO i, TEMOS $x - y \equiv 0 \pmod{m_i}$
ISSO É, $x-y$ É MÚLTIPLO DE m_i PARA TODO i.
COMO $m_i \perp m_j$, $x-y$ É MÚLTIPLO DE $m_1 \cdots m_k = m$.
OU SEJA, $x \equiv y \pmod{m}$. □