de chinese reststelling

Veronderstel dat m_1, ... ,m_k positieve natuurlijke getallen zijn die 2 aan 2 onderling ondeelbaar zijn m.a.w. gcd(m_i, m_j)=1 als i $\neq$ j.

$$Zij\ M = \prod_{i=1}^{k} m_i = m_1 \cdots m_k.$$

Beschouw verder voor elke i een b_i ∊ N[0, m_i-1]. Dan heeft het stelsel lineaire congruenties

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \quad \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

juist 1 oplossing modulo M

bewijs
beshouw de afbeelding

$$\theta\colon \begin{array}{l} \mathbb{Z}/M \to \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_k\colon \\ \;[t]_M \mapsto ([t]_{m_1}, \ldots, [t]_{m_k}). \end{array}$$

Deze afbeelding is goed gedefinieerd, d.w.z. dat de uitrdukking ($[t]_{m1}$, ... ,$[t]_{mk}$) onafhankelijk is van de keuze van de representant t ∊Z voor het element $[t]_M$ ∊Z/M. inderdaad, veronderstel dat s $\equiv$ t (mod m); dan is M ∣ s-t , en bijgevolg is m_i ∣ s-t, dwz s$\equiv$ t(mod m_i) voor elke i ∊ {1, 2, ... , k}.

Vervolgens gaan we na dat deze afbeelding injectief is. Indrdaad, veronderstel dat s, t ∊Z zodanig zijn dat θ ($[s]_m$) = θ ($[t]_m$). dan is s$\equiv$ t (mod m_i) en dus m_i ∣ s-t voor elke i ∊{1, ... ,k}.
Omdat de m_i's onderling ondeelbaar zijn, volgt uit de stelling stelling 6.2.5 nu dat M∣s-t, en dus is s$\equiv$ t (mod M). Hieruit volgt dat θ injectief is.
Merk nu op dat Z/M en Z/m_1 x ... x Z/m_k evenveel elementen bevatten (namelijk M).

Een injectie tussen 2 verzamelingen die dezelfde eindige kardinaliteit hebben, is echter noodzakelijk een bijectie, en dus besluiten we dat θ een bijectie is.
In het bijzonder is err juist één element $[t]_M$ ∊ Z/M waarvoor
θ($[t]_M$) = ($[b_1]_{m1}$, ... , $[b_k]_{mk}$)
en dat is wat we wilden bewijzen