Beweis des Chinesischen Restsatzes

Beob Wenn ich Paar (k,l) von Unterschiedl. Indizes habe, dann

$$I_k + I_l = R, \text{ also } \exists\ a_{kl} \in I_k,\ b_{kl} \in I_l \text{ s.d. } 1 = a_{kl} + b_{kl} \text{ ist.}$$

Dann setze für jeden Index l

$$S_l = \prod_{k \neq l} a_{kl} \quad (a_{kl} \in I_k) \quad = \prod_{k \neq l} (1 - b_{kl}) \quad (1 - b_{kl} \in I_l)$$

Dann gilt

① $S_l \in I_k$ für alle $k \neq l$

② $S_l \equiv 1 \pmod{I_l}$

Jetzt zum Beweis:

- Aussage zum hirn ist trivial ✓
- Gegeben $r_1, \dots, r_n$. Setze $r = \sum_l S_l \cdot r_l$

  Dann gilt $\forall k$: $\quad r = S_k \cdot r_k + \sum_{l \neq k} S_l \cdot r_l$

  $S_k \equiv 1 \pmod{I_k}$, $\sum_{l \neq k} S_l \cdot r_l \equiv 0 \pmod{I_k}$

  Also $\quad r \equiv 1 \cdot r_k \pmod{I_k}$

Damit ist das gesuchte Elt. r gefunden. □