27. chinesischer Restsatz

Satz: Es seien m, n teilerfremd und $k, l \in \mathbb{N}$.
Dann gilt es genau eine Zahl $x \in \{0, ..., mn - 1\}$ mit
$1 \equiv k \ mod \ m$
$1 \equiv l \ mod \ b$

Beweis: Nach Bézout gibt es $a, b \in \mathbb{Z}$ dass $a \cdot m + b \cdot n = 1$.
Behauptung: $x := l \cdot a \cdot m + k \cdot b \cdot n$
leistet die gewünschte:
$lam + kbn \equiv (q - am)k \equiv k \ mod \ m$
$lam + kbn \equiv lam \equiv (1 - bn)l \equiv l \ mod \ n$