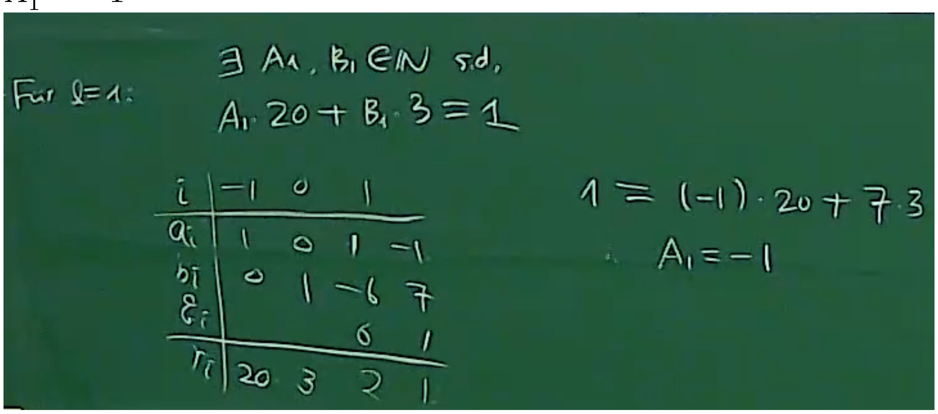
- gesucht Menge aller Lösungen x∈$\mathbb{Z}$ der simultanen Kongruenzen
  - $x \equiv c_1 \bmod m_1$
  - $x \equiv c_2 \bmod m_2$
  - ...
  - $x \equiv c_n \bmod m_n$
- Vorgehensweise
  - m_1 bis m_n sind teilerfremd
    - ansonsten redundante Kongruenzen eliminieren
  - Produkt berechnen
    - $M = \prod_{i=1}^{n} a_i$
  - $M_i = \frac{M}{m_i}$
  - euklidischen Alg. anwenden
    - $a_i * m_i + b_i * M_i = 1$
  - Lösung
    - $x = \sum_{i=1}^{n} x_i * s_i * Ai$
    - Falls a∉{0,...,m-1}, b∈{0,...,m-1} sodass a≡b mod m
      - $L =\{x \in \mathbb{Z} : x \equiv C_l \bmod m_l \ \forall l = 1...s\} = [b]_m = [a]_m$
- Beispiel:
  - gegeben:
    - $c_1 = 1, c_2 = 2, c_3 = 3$
    - $m_1 = 3, m_2 = 4, m_3 = 5$
  - $m = 3 * 4 * 5 = 60$
  - euklidische Alg.
    - l=1
      - $A_1 = -1$
      - 

    - l=2
      - $A_2 = -1$
    - l=3

        - $A_3 = -2$
- $x = \sum_{l=1}^{3} C_l * A_l * n_l = 1(-1)20 + 2(-1)15 + 3(-2)12 = -122$
    - n_l ist Produkt aller m außer m_l
    - $x \equiv -122 mod 60 ==> x \equiv 58 mod 60$
    - Lösungsmenge $[58]_6 0$

[[Diskrete Mathematik]]