

לעבור ל- m_i בלבד ולכן $m_i \in \mathbb{Z}_{u_i}^*$ ויש לנו $\gcd(m_i, u_i) = 1$ ולכן m_i^{-1} קיים

$C_r(a) = (a_1, \dots, a_k)$ ויש לנו $a = (a_1 c_1 + \dots + a_k c_k) \pmod{u}$ ויש לנו

$a \equiv a_i \pmod{u_i} \quad 1 \leq i \leq k$ ולכן

$$a \pmod{u_i} = ((a_1 c_1 + \dots + a_k c_k) \pmod{u}) \pmod{u_i} = (a_1 c_1 + \dots + a_k c_k) \pmod{u_i} = (*)$$

$$a_j c_j \pmod{u_i} = a_j m_j x \pmod{u_i} = 0 \quad i \neq j \quad \text{כי}$$

ל- u_i ול- m_j אין גורם משותף

$$(*) = a_i c_i \pmod{u_i} = a_i m_i m_i^{-1} \pmod{u_i} = a_i$$

כל $\mathbb{Z}_{u_i}^*$ ויש לנו
כל $\mathbb{Z}_{u_i}$ ויש לנו

לכן

$$n=12 \quad u_1=3 \quad u_2=4 \quad \text{ולכן } (2,1) \text{ ו-}(1,3)$$

$$c_1=4 \quad c_2=9 \quad \text{כל } m_1^{-1}=1 \quad m_2^{-1}=3 \quad , \quad m_1=4 \quad m_2=3 \quad \text{ולכן}$$

$$(2 \cdot 4 + 1 \cdot 9) = 17 = 5 \pmod{12}$$

$$C_r(5) = (2,1) \quad \text{כל}$$

הוכחה של תוצאה

$n = p \cdot q$ ויש לנו p, q ראשוניים

$0 \leq m \leq n-1$ ויש לנו m ויש לנו p, q ראשוניים

$$C = C(m) = m^2 \pmod{n}$$

$$m_q = C^{\frac{q+1}{4}} \pmod{q} \quad m_p = C^{\frac{p+1}{4}} \pmod{p}$$

$$1. \quad m_p^2 \equiv C^{\frac{p+1}{2}} \equiv m^{p+1} \equiv m^2 m^{p-1} \equiv m^2$$

לכן

$$2. \quad m_q^2 \equiv m^2$$

לכן