

סימן יזקובי

$$m = p_1 \dots p_k$$

$m \in \mathbb{N}$  אי-זוגי, נפרק  
 $p_i$  ראשוני אי-זוגי (מותר זוגי)  
 $a \in \mathbb{Z}_m^*$  מסומים

הקדמה - אם  
כאשר  
אם

$$\left(\frac{a}{m}\right) = \prod_{i=1}^k \left(\frac{a}{p_i}\right)$$

בנו סימן יזקובי

$$\left(\frac{a}{m}\right) = 0 \text{ נכון } \gcd(a, m) \geq 1 \text{ אם}$$

הערות

אם  $m = p$  ראשוני אי-זוגי אז סימן יזקובי מסומים מתחילים

$$\left(\frac{a}{m}\right) = i \leftarrow \exists x, x^2 \equiv a \pmod{m} \leftarrow \exists x, x^2 \equiv a \pmod{p_i} \leftarrow \exists x, \left(\frac{a}{p_i}\right) = 1$$

3) ההיפך אינו בהכרח נכון.

$$\left(\frac{2}{105}\right) = \left(\frac{2}{3}\right) \left(\frac{2}{5}\right) \left(\frac{2}{7}\right) = (-1)(-1) \cdot 1 = 1$$

דוגמה -

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, p \equiv \pm 1 \pmod{8} \\ -1, \text{ אחרת} \end{cases}$$

לפי קיים פיתרון  $x^2 \equiv 2 \pmod{105}$  כי לפי קיים פתרון  $x^2 \equiv 2 \pmod{3}$

כמות סימן יזקובי

ל"ח  $m, n$  גזיים אי-זוגיים, אז:

$$\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right) \quad (1) \text{ אם } a, b \text{ זרים ל-} m$$

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right) \quad (2) \text{ אם } a \text{ זר ל-} m \text{ ו-} n$$

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} \quad (3)$$

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} \quad (4)$$

$$\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = (-1)^{\frac{1}{4}(m-1)(n-1)} \quad (5)$$

$$\left(\frac{1711}{997}\right) = \left(\frac{714}{997}\right) = \left(\frac{2}{997}\right) \left(\frac{357}{997}\right) =$$

דוגמה -

בזקיים  $u = 2, 357$  זרים לפי האלגוריתם האוקלידי

$$997 \equiv -3 \pmod{8} \rightarrow - \left(\frac{357}{997}\right) = (-1)^{\frac{1}{4}(356 \cdot 966)} \left(\frac{997}{357}\right) = - \left(\frac{283}{357}\right) =$$

$$= - \left(\frac{357}{283}\right) (-1)^{\frac{1}{4} \cdot 356 \cdot 282} = - \left(\frac{74}{283}\right) = - \left(\frac{2}{283}\right) \left(\frac{37}{283}\right) = \left(\frac{283}{37}\right) (-1)^{\frac{1}{4} \cdot 36 \cdot 282} = \left(\frac{24}{37}\right) =$$
  
$$= \left(\frac{2}{37}\right) \left(\frac{3}{37}\right) \left(\frac{3}{37}\right) \left(\frac{3}{37}\right) = - \left(\frac{37}{3}\right) = -\frac{1}{3} = -1$$

הוכחה

(1) הוכחנו מקור מ ראשוני, וסוף :

$$\left(\frac{ab}{m}\right) = \left(\frac{ab}{p_1}\right) \dots \left(\frac{ab}{p_k}\right) = \left(\frac{a}{p_1}\right) \left(\frac{b}{p_1}\right) \dots \left(\frac{a}{p_k}\right) \left(\frac{b}{p_k}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_k}\right) \left(\frac{b}{p_1}\right) \dots \left(\frac{b}{p_k}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right)$$

$$mn = p_1 \dots p_k q_1 \dots q_l, \quad n = q_1 \dots q_l, \quad m = p_1 \dots p_k \quad (2)$$

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_k}\right) \left(\frac{a}{q_1}\right) \dots \left(\frac{a}{q_l}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$$

(3) מוכיחים באינדוקציה על האורך ק בסדר  $m = p_1 \dots p_k$

נניח  $m = m_1 \cdot m_2$ ,  $m_1 = p_1 \dots p_{k-1}$ ,  $m_2 = p_k$  יציבים

נניח  $m_1, m_2$  זוגי 3-ש

$$\left(\frac{-1}{m}\right) = \left(\frac{-1}{m_1}\right) \left(\frac{-1}{m_2}\right) = (-1)^{\frac{1}{2}(m_1-1)} \cdot (-1)^{\frac{1}{2}(m_2-1)} = (-1)^{\frac{1}{2}(m_1+m_2-2)}$$

לפיכך -  $m_1, m_2$  יציבים  $\frac{(m-1)(m-2)}{2}$

$$\frac{1}{2}(m_1, m_2 - m_1 - m_2 + 1) = \frac{1}{2}(m_1 - 1)(m_2 - 1) \equiv 0 \pmod{2}$$

$$\frac{1}{2}(m-1 - (m_1+m_2) + 2) = \frac{1}{2}(m-1) - \left[\frac{1}{2}(m_1-1) + \frac{1}{2}(m_2-1)\right]$$

$$(-1)^{\frac{1}{2}(m-1)} = (-1)^{\frac{1}{2}[m_1-1+m_2-1]}$$

$$n = q_1 \dots q_l, \quad m = p_1 \dots p_k \quad (5)$$

$$\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = \left(\frac{p_1}{n}\right) \dots \left(\frac{p_k}{n}\right) \left(\frac{q_1}{m}\right) \dots \left(\frac{q_l}{m}\right) = \prod_{\substack{i=1 \dots k \\ j=1 \dots l}} \left(\frac{p_i}{q_j}\right) \left(\frac{q_j}{p_i}\right) =$$

$$= \prod_{i,j} (-1)^{\frac{1}{2}(p_i-1) \cdot \frac{1}{2}(q_j-1)} =$$

$$= (-1)^{\sum_{i,j} \frac{1}{2}(p_i-1) \frac{1}{2}(q_j-1)} = (-1)^{\sum_i \frac{1}{2}(p_i-1) \sum_j \frac{1}{2}(q_j-1)} =$$

$$= \left((-1)^{\sum_i \frac{1}{2}(p_i-1)}\right)^{\sum_j \frac{1}{2}(q_j-1)} = \left((-1)^{\frac{1}{2}(m-1)}\right)^{\sum_j \frac{1}{2}(q_j-1)} =$$

$$= \left((-1)^{\frac{1}{2}(m-1)}\right)^{\frac{1}{2}(n-1)} = (-1)^{\frac{1}{2}(m-1)(n-1)} = (-1)^{\frac{1}{2}(n-1)(m-1)}$$