

סימן יעקובי

$$m = p_1 \dots p_k$$

$m \in \mathbb{N}$ איז-צ'י, נפרק
 p_i ראשוני איצ'י (מותר ריבוי)
 $a \in \mathbb{Z}_m^*$ מסתמים

הגדרה - אם
 כאשר
 אם

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

בנו **סימן יעקובי**

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

הערות

(1) אם $m = p$ ראשוני אז סימן יעקובי מתכנס

(2) אם a מסתמים ראשוני m , אז קיים x כך ש-
 $x^2 \equiv a \pmod{m} \iff x^2 \equiv a \pmod{p_i} \iff \left(\frac{a}{p_i}\right) = 1$ $\iff \left(\frac{a}{m}\right) = 1$

(3) ההיפך אינו בהכרח נכון.

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

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

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

כיוונון סימן יעקובי

נ"ח m, n גז"מ איז צ'י, אז:
 (1) אם a, b צ'ים m אז $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right)$

(2) אם a זר m אז $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$

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

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

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

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

בזקיים $2, 357$ זרים לפי האלגוריתם האוקלידי

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

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

$$= \left(\frac{2}{37}\right) \left(\frac{37}{37}\right) \left(\frac{3}{37}\right) \left(\frac{3}{37}\right) = -\left(\frac{37}{3}\right) = -\frac{1}{3} = -1$$

הוכחה

(1) הוכחנו מקור m ראשוני, וכן:

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

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

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

(3) מניחים באינדוקציה על האורך k בערך $m = p_1 \cdots p_k$

$$m = m_1 m_2, \quad m_1 = p_1 \cdots p_{k-1}, \quad m_2 = p_k$$

נניח m_1, m_2 זוגי 3-ש

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

מכאן m_1, m_2 זוגי 2-ש

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

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

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

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

$$\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = \left(\frac{p_1}{q_1}\right) \cdots \left(\frac{p_k}{q_l}\right) \left(\frac{q_1}{p_1}\right) \cdots \left(\frac{q_l}{p_k}\right) = \prod_{i=1}^k \left(\frac{p_i}{q_i}\right) \left(\frac{q_i}{p_i}\right) =$$

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

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

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

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