



วารสารคณิตศาสตร์ **Mathematical Journal** 64(699) กันยายน – ธันวาคม 2562

โดย สมาคมคณิตศาสตร์แห่งประเทศไทย ในพระบรมราชูปถัมภ์

<http://www.mathassociation.net>

Email: MathThaiOrg@gmail.com

รูปแบบจำนวนเฉพาะคือ p ในสัญลักษณ์เลอจองด์ ($2p_1p_2 / p$)

Forms of Odd Prime Numbers p in Legendre Symbol ($2p_1p_2 / p$)

อภิรัฐ ศิระวรกุล

Apirat Siraworakun

Program of Mathematics, Faculty of Science and Technology,
Thepsatri Rajabhat University, Lopburi 15000

Email: nookkop2525@gmail.com

วันที่รับบทความ : 4 กรกฎาคม 2562

วันที่แก้ไขบทความ : 8 สิงหาคม 2562

วันที่ตอบรับบทความ : 22 สิงหาคม 2562

บทคัดย่อ

ในงานวิจัยนี้ เราได้ศึกษารูปแบบจำนวนเฉพาะคือ p ในสัญลักษณ์เลอจองด์ ($2p_1p_2 / p$) เมื่อ p_1, p_2 เป็นจำนวนเฉพาะคือ $p \nmid p_1$ และ $p \nmid p_2$ โดยใช้ทฤษฎีบทเศษเหลือของจีนในการหาผลเฉลี่ยของระบบสมภาค เราแบ่งการศึกษานี้ออกเป็น 3 กรณี ดังต่อไปนี้

1. $p_1 \equiv 1 \pmod{4}$ และ $p_2 \equiv 1 \pmod{4}$

2. $p_1 \equiv 1 \pmod{4}$ และ $p_2 \equiv 3 \pmod{4}$

3. $p_1 \equiv 3 \pmod{4}$ และ $p_2 \equiv 3 \pmod{4}$

คำสำคัญ: ส่วนตกค้างกำลังสอง สัญลักษณ์เลอจองด์ ทฤษฎีบทเศษเหลือของจีน

ABSTRACT

In this research, we study the form of odd prime number p in Legendre Symbol $(2p_1p_2/p)$ where p_1, p_2 are odd prime numbers, $p \nmid p_1$ and $p \nmid p_2$ by using Chinese Remainder Theorem for finding the solutions of system of congruence. We separate this study into 3 cases as the followings.

1. $p_1 \equiv 1 \pmod{4}$ and $p_2 \equiv 1 \pmod{4}$
2. $p_1 \equiv 1 \pmod{4}$ and $p_2 \equiv 3 \pmod{4}$
3. $p_1 \equiv 3 \pmod{4}$ and $p_2 \equiv 3 \pmod{4}$

Keywords: Quadratic Residue, Legendre Symbol, Chinese Remainder Theorem

1. บทนำ

สำหรับจำนวนเต็มบวก m และจำนวนเต็ม a ที่ $(a, m) = 1$ เราจะกล่าวว่า a เป็นส่วนตกค้างกำลังสองมอดุโล m ก็ต่อเมื่อ $x^2 \equiv a \pmod{m}$ มีผลเฉลย

สัญลักษณ์เลอจองด์เป็นสัญลักษณ์ที่แสดงถึงความเป็นส่วนตกค้างกำลังสองซึ่งนิยามดังต่อไปนี้

บทนิยาม 1.1 [1] กำหนดให้ p เป็นจำนวนเฉพาะคี่ และ a เป็นจำนวนเต็มที่ $p \nmid a$ สัญลักษณ์เลอจองด์ (Legendre symbol) (a/p) จะกำหนดค่าให้ได้ดังนี้

$(a/p) = 1$ เมื่อ a เป็นส่วนตกค้างกำลังสอง มอดุโล p

$(a/p) = -1$ เมื่อ a ไม่เป็นส่วนตกค้างกำลังสอง มอดุโล p

สำหรับกรณีที่ $a = 2$ อัจฉรา หาญชูวงศ์ [1] ได้กล่าวถึงรูปแบบของจำนวนเฉพาะคี่ในสัญลักษณ์เลอจองด์ไว้ดังนี้

$$(2/p) = \begin{cases} 1, & p \equiv \pm 1 \pmod{8} \\ -1, & p \equiv \pm 3 \pmod{8} \end{cases}$$

จากการศึกษางานวิจัยที่เกี่ยวข้องกับการหารูปแบบจำนวนเฉพาะคี่ในสัญลักษณ์เลอจองด์ พบว่าในปี พ.ศ. 2547 อภิรัฐ ศิริวรกุล [2] ได้ศึกษาหารูปแบบของจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ (b/p) เมื่อ b เป็นจำนวนเฉพาะคี่ ที่ $p \nmid b$ ซึ่งมีผลการวิจัยดังนี้

ทฤษฎีบท 1.1 [2] กำหนดให้ b และ p เป็นจำนวนเฉพาะที่ โดยที่ $p \nmid b$ และ $b \equiv 1 \pmod{4}$ จะได้ว่า

$$(b/p) = \begin{cases} 1, & p \equiv b + r^{S_1}b + r^{S_1} \pmod{2b} \\ -1, & p \equiv b + r^{T_1}b + r^{T_1} \pmod{2b} \end{cases}$$

เมื่อ $S_1 \in \{2, 4, 6, \dots, b-1\}$, $T_1 \in \{1, 3, 5, \dots, b-2\}$ และ r เป็นรากปฐมฐานมอดุโล b

ทฤษฎีบท 1.2 [2] กำหนดให้ b และ p เป็นจำนวนเฉพาะที่ โดยที่ $p \nmid b$ และ $b \equiv 3 \pmod{4}$ จะได้ว่า

$$(b/p) = \begin{cases} 1, & p \equiv 3b + 4n_0r^{S_1} \pmod{4b}, \\ & \equiv -3b + 4n_0r^{T_1} \pmod{4b} \\ -1, & p \equiv 3b + 4n_0r^{T_1} \pmod{4b}, \\ & \equiv -3b + 4n_0r^{S_1} \pmod{4b} \end{cases}$$

เมื่อ $S_1 \in \{2, 4, 6, \dots, b-1\}$, $T_1 \in \{1, 3, 5, \dots, b-2\}$, n_0 เป็นจำนวนนับ และ r เป็นรากปฐมฐานมอดุโล b โดยที่ n_0 สอดคล้องกับสมการ $b = 4n_0 - 1$

ในปี พ.ศ. 2559 อภิรัฐ ศิระวรกุล และคณะ [3] ได้ศึกษารูปแบบจำนวนเฉพาะที่ p ในสัญลักษณ์เลอจองต์ (p_1p_2 / p) เมื่อ p_1 และ p_2 เป็นจำนวนเฉพาะที่ ซึ่ง $p \nmid p_1$ และ $p \nmid p_2$ ซึ่งมีผลวิจัยดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 1.3 [3] กำหนดให้ p_1, p_2 และ p เป็นจำนวนเฉพาะที่ ซึ่ง $p_1 \equiv 1 \pmod{4}$, $p_2 \equiv 1 \pmod{4}$, $p \nmid p_1$ และ $p \nmid p_2$ จะได้ว่า

$$(p_1p_2/p) = \begin{cases} 1, & p \equiv p_1p_2 + 2(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{2p_1p_2}, \\ & \equiv p_1p_2 + 2(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{2p_1p_2} \\ -1, & p \equiv p_1p_2 + 2(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{2p_1p_2}, \\ & \equiv p_1p_2 + 2(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{2p_1p_2} \end{cases}$$

เมื่อ $S_1 \in \{2, 4, 6, \dots, p_1-1\}$, $S_2 \in \{2, 4, 6, \dots, p_2-1\}$, $T_1 \in \{1, 3, 5, \dots, p_1-2\}$,

$T_2 \in \{1, 3, 5, \dots, p_2 - 2\}$, r_1 และ r_2 เป็นรากปฐมฐานมอดุโล p_1 และ p_2 ตามลำดับ และ n_1 และ n_2 เป็นจำนวนเต็มสอดคล้องกับ $2p_2n_1 \equiv 1 \pmod{p_1}$ และ $2p_1n_2 \equiv 1 \pmod{p_2}$ ตามลำดับ

ทฤษฎีบท 1.4 [3] กำหนดให้ p_1, p_2 และ p เป็นจำนวนเฉพาะคี่ ซึ่ง $p_1 \equiv 1 \pmod{4}$, $p_2 \equiv 3 \pmod{4}$, $p \nmid p_1$ และ $p \nmid p_2$ จะได้ว่า

$$(p_1p_2 / p) \equiv \begin{cases} 1, & p \equiv -p_1p_2 + 4(n_3r_1^{S_1}p_2 + 4n_0n_4r_2^{S_2}p_1) \pmod{4p_1p_2}, \\ & \equiv p_1p_2 + 4(n_3r_1^{S_1}p_2 + 4n_0n_4r_2^{T_2}p_1) \pmod{4p_1p_2}, \\ & \equiv -p_1p_2 + 4(n_3r_1^{T_1}p_2 + 4n_0n_4r_2^{T_2}p_1) \pmod{4p_1p_2}, \\ & \equiv p_1p_2 + 4(n_3r_1^{T_1}p_2 + 4n_0n_4r_2^{S_2}p_1) \pmod{4p_1p_2} \\ -1, & p \equiv -p_1p_2 + 4(n_3r_1^{T_1}p_2 + 4n_0n_4r_2^{S_2}p_1) \pmod{4p_1p_2}, \\ & \equiv p_1p_2 + 4(n_3r_1^{T_1}p_2 + 4n_0n_4r_2^{T_2}p_1) \pmod{4p_1p_2}, \\ & \equiv -p_1p_2 + 4(n_3r_1^{S_1}p_2 + 4n_0n_4r_2^{T_2}p_1) \pmod{4p_1p_2}, \\ & \equiv p_1p_2 + 4(n_3r_1^{S_1}p_2 + 4n_0n_4r_2^{S_2}p_1) \pmod{4p_1p_2} \end{cases}$$

เมื่อ $S_1 \in \{2, 4, 6, \dots, p_1 - 1\}$, $S_2 \in \{2, 4, 6, \dots, p_2 - 1\}$, $T_1 \in \{1, 3, 5, \dots, p_1 - 2\}$,

$T_2 \in \{1, 3, 5, \dots, p_2 - 2\}$, r_1 และ r_2 เป็นรากปฐมฐานมอดุโล p_1 และ p_2 ตามลำดับ และ n_0, n_3 และ n_4 เป็นจำนวนเต็มที่สอดคล้อง $p_2 = 4n_0 - 1$, $4p_2n_3 \equiv 1 \pmod{p_1}$ และ $4p_1n_4 \equiv 1 \pmod{p_2}$ ตามลำดับ

ทฤษฎีบท 1.5 [3] กำหนดให้ p_1, p_2 และ p เป็นจำนวนเฉพาะคี่ ซึ่ง $p_1 \equiv 3 \pmod{4}$, $p_2 \equiv 3 \pmod{4}$, $p \nmid p_1$ และ $p \nmid p_2$ จะได้ว่า

$$(p_1p_2 / p) \equiv \begin{cases} 1, & \begin{aligned} p &\equiv p_1p_2 + 16(n_0n_3r_1^{S_1}p_2 + m_0n_4r_2^{S_2}p_1) \pmod{4p_1p_2}, \\ &\equiv -p_1p_2 + 16(n_0n_3r_1^{T_1}p_2 + m_0n_4r_2^{T_2}p_1) \pmod{4p_1p_2}, \\ &\equiv p_1p_2 + 16(n_0n_3r_1^{T_1}p_2 + m_0n_4r_2^{T_2}p_1) \pmod{4p_1p_2}, \\ &\equiv -p_1p_2 + 16(n_0n_3r_1^{S_1}p_2 + m_0n_4r_2^{S_2}p_1) \pmod{4p_1p_2} \end{aligned} \\ -1, & \begin{aligned} p &\equiv p_1p_2 + 16(n_0n_3r_1^{T_1}p_2 + m_0n_4r_2^{S_2}p_1) \pmod{4p_1p_2}, \\ &\equiv -p_1p_2 + 16(n_0n_3r_1^{S_1}p_2 + m_0n_4r_2^{T_2}p_1) \pmod{4p_1p_2}, \\ &\equiv p_1p_2 + 16(n_0n_3r_1^{S_1}p_2 + m_0n_4r_2^{T_2}p_1) \pmod{4p_1p_2}, \\ &\equiv -p_1p_2 + 16(n_0n_3r_1^{T_1}p_2 + m_0n_4r_2^{S_2}p_1) \pmod{4p_1p_2} \end{aligned} \end{cases}$$

เมื่อ $S_1 \in \{2, 4, 6, \dots, p_1 - 1\}$, $S_2 \in \{2, 4, 6, \dots, p_2 - 1\}$, $T_1 \in \{1, 3, 5, \dots, p_1 - 2\}$,

$T_2 \in \{1, 3, 5, \dots, p_2 - 2\}$, r_1 และ r_2 เป็นรากปฐมนฐานมอดุโล p_1 และ p_2 ตามลำดับ และ n_0, m_0, n_3 และ n_4 เป็นจำนวนเต็มที่สุดคัล้อง $p_1 = 4n_0 - 1$, $p_2 = 4m_0 - 1$,

$4p_2n_3 \equiv 1 \pmod{p_1}$ และ $4p_1n_4 \equiv 1 \pmod{p_2}$ ตามลำดับ

จากสิ่งที่กล่าวมาข้างต้น ทำให้ผู้วิจัยได้ต่อยอดแนวความคิดนี้ โดยพิจารณาหารูปแบบของจำนวนเฉพาะที่ p ในสัญลักษณ์เลอจองด์ ($2p_1p_2 / p$) เมื่อ p_1, p_2 เป็นจำนวนเฉพาะที่, $p \nmid p_1$ และ $p \nmid p_2$

2. ผลการวิจัย

ในงานวิจัยนี้ ทฤษฎีบทเศษเหลือของจีนถือได้ว่าเป็นเครื่องมือสำคัญในการแก้ระบบสมภาคเพื่อหารูปแบบจำนวนเฉพาะที่ในสัญลักษณ์เลอจองด์ โดยทฤษฎีบทเศษเหลือของจีนมีเนื้อความดังต่อไปนี้

ทฤษฎีบท 2.1 [1] กำหนดให้ $m_1, m_2, m_3, \dots, m_n$ เป็นจำนวนเต็มบวกที่เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ และ $a_1, a_2, a_3, \dots, a_n$ เป็นจำนวนเต็มใด ๆ จะได้ว่าระบบสมภาค

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_n \pmod{m_n}$$

จะมีผลเฉลยเพียงตัวเดียวมอดุโล m เมื่อ $m = m_1 m_2 m_3 \dots m_n$ นั่นคือ มี x_0 เป็นผลเฉลย และผลเฉลยทั้งหมดจะอยู่ในรูป $x_0 + km$ เมื่อ k เป็นจำนวนเต็มใด ๆ

ในบทพิสูจน์ของทฤษฎีบทเศษเหลือของจีนได้กล่าวถึงรูปแบบผลเฉลยของระบบสมภาคไว้ดังนี้

$$a_1 m'_1 y_1 + a_2 m'_2 y_2 + a_3 m'_3 y_3 + \dots + a_n m'_n y_n$$

เมื่อ $m'_i = \frac{m}{m_i}$ และ y_i หาได้จาก $m'_i y_i \equiv 1 \pmod{m_i}$ ทุก $i \in \{1, 2, 3, \dots, n\}$

นอกเหนือจากทฤษฎีเศษเหลือของจีนแล้ว เรายังใช้ทฤษฎีบทต่อไปนี้ในการพิสูจน์เพื่อหารูปแบบจำนวนเฉพาะคี่ในสัญลักษณ์เลขจอตด้วย

ทฤษฎีบท 2.2 [1] กำหนดให้ $m_1, m_2, m_3, \dots, m_n$ เป็นจำนวนเต็มบวก และ $b_1, b_2, b_3, \dots, b_n$ ที่เป็นจำนวนเต็มใด ๆ จะได้ว่าระบบสมภาค

$$x \equiv b_1 \pmod{m_1}$$

$$x \equiv b_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv b_n \pmod{m_n}$$

จะมีผลเฉลย ก็ต่อเมื่อ $(m_i, m_j) | (b_i - b_j)$ สำหรับทุกค่า $i, j \in \{1, 2, 3, \dots, n\}$ ที่ $i \neq j$ และถ้ามีผลเฉลย จะมีผลเฉลยเพียงตัวเดียวมอดุโล $[m_1, m_2, m_3, \dots, m_n]$

ทฤษฎีบท 2.3 [1] กำหนดให้ p เป็นจำนวนเฉพาะคี่ และ a, b เป็นจำนวนเต็มที่ $p \nmid a$ และ $p \nmid b$ จะได้ว่า $(ab/p) = (a/p)(b/p)$

สำหรับการศึกษาหารูปแบบของจำนวนเฉพาะคี่ p ในสัญลักษณ์เลขจอต $(2p_1 p_2 / p)$ เมื่อ p_1, p_2 เป็นจำนวนเฉพาะคี่, $p \nmid p_1$ และ $p \nmid p_2$ เราได้แบ่งการศึกษาออกเป็น 3 กรณี ดังต่อไปนี้

$$1. \quad p_1 \equiv 1 \pmod{4} \text{ และ } p_2 \equiv 1 \pmod{4}$$

$$2. \quad p_1 \equiv 1 \pmod{4} \text{ และ } p_2 \equiv 3 \pmod{4}$$

$$3. \quad p_1 \equiv 3 \pmod{4} \text{ และ } p_2 \equiv 3 \pmod{4}$$

กรณีที่ 1 $p_1 \equiv 1 \pmod{4}$ และ $p_2 \equiv 1 \pmod{4}$

ทฤษฎีบท 2.4 ให้ p_1 และ p_2 เป็นจำนวนเฉพาะคี่ที่ทำให้มีจำนวนเต็ม m และ n ซึ่งสอดคล้องกับ $p_1 = 4m+1$ และ $p_2 = 4n+1$ จะได้ว่า

1. ถ้า $m+n$ เป็นจำนวนเต็มคู่ แล้ว $p_1p_2 \equiv 1 \pmod{8}$
2. ถ้า $m+n$ เป็นจำนวนเต็มคี่ แล้ว $-3p_1p_2 \equiv 1 \pmod{8}$

บทพิสูจน์

1. สมมติ $m+n$ เป็นจำนวนเต็มคู่ จะมีจำนวนเต็ม l ที่ทำให้ $m+n=2l$ เพราะฉะนั้น

$$p_1p_2 = (4m+1)(4n+1) = 16mn + 4(m+n) + 1 = 16mn + 4(2l) + 1 = 8(2mn+l) + 1 \text{ ดังนั้น}$$

$$p_1p_2 \equiv 1 \pmod{8}$$

2. สมมติ $m+n$ เป็นจำนวนเต็มคี่ จะมีจำนวนเต็ม l ที่ทำให้ $m+n=2l+1$ จะได้ว่า

$$p_1p_2 = (4m+1)(4n+1) = 16mn + 4(m+n) + 1 = 16mn + 4(2l+1) + 1 = 8(2mn+l) + 5$$

เพราะฉะนั้น

$$-3p_1p_2 = 8(-6mn-3l) - 15 = 8(-6mn-3l) - 16 + 1 = 8(-6mn-3l-2) + 1$$

$$\text{ดังนั้น } -3p_1p_2 \equiv 1 \pmod{8}$$

□

ทฤษฎีบท 2.5 ให้ p_1 , p_2 และ p เป็นจำนวนเฉพาะคี่ ซึ่ง $p \nmid p_1$ และ $p \nmid p_2$ และ

ถ้า $p_1 = 4m+1$ และ $p_2 = 4n+1$ สำหรับบางจำนวนเต็ม m และ n จะได้ว่า

1. ถ้า $m+n$ เป็นจำนวนเต็มคู่ แล้ว

$$(2p_1p_2 / p) = \begin{cases} 1, & \begin{aligned} p &\equiv p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2} \end{aligned} \\ -1, & \begin{aligned} p &\equiv p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2} \end{aligned} \end{cases}$$

เมื่อ $S_1 \in \{2, 4, 6, \dots, p_1 - 1\}$, $S_2 \in \{2, 4, 6, \dots, p_2 - 1\}$, $T_1 \in \{1, 3, 5, \dots, p_1 - 2\}$, $T_2 \in \{1, 3, 5, \dots, p_2 - 2\}$, r_1 และ r_2 เป็นรากปฐมฐานมอดุโล p_1 และ p_2 ตามลำดับ และ n_1, n_2 และ n_3 เป็นจำนวนเต็มสอดคล้องกับ $2p_2n_1 \equiv 1 \pmod{p_1}$, $2p_1n_2 \equiv 1 \pmod{p_2}$ และ $8n_3 \equiv 1 \pmod{p_1p_2}$ ตามลำดับ

2. ถ้า $m+n$ เป็นจำนวนเต็มคี่ แล้ว

$$(2p_1p_2 / p) = \begin{cases} 1, & \begin{aligned} p &\equiv -3p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2} \end{aligned} \\ -1, & \begin{aligned} p &\equiv -3p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2} \end{aligned} \end{cases}$$

เมื่อ $S_1 \in \{2, 4, 6, \dots, p_1 - 1\}$, $S_2 \in \{2, 4, 6, \dots, p_2 - 1\}$, $T_1 \in \{1, 3, 5, \dots, p_1 - 2\}$
 $T_2 \in \{1, 3, 5, \dots, p_2 - 2\}$, r_1 และ r_2 เป็นรากปฐมนฐานมอดุโล p_1 และ p_2 ตามลำดับ และ
 n_1, n_2 และ n_3 เป็นจำนวนเต็มสอดคล้องกับ $2p_2n_1 \equiv 1 \pmod{p_1}$, $2p_1n_2 \equiv 1 \pmod{p_2}$
 และ $8n_3 \equiv 1 \pmod{p_1p_2}$ ตามลำดับ

กรณีที่ 2 $p_1 \equiv 1 \pmod{4}$ และ $p_2 \equiv 3 \pmod{4}$

ทฤษฎีบท 2.6 ให้ p_1 และ p_2 เป็นจำนวนเฉพาะคี่ที่ทำให้มีจำนวนเต็ม m และ n ซึ่งสอดคล้องกับ $p_1 = 4m + 1$ และ $p_2 = 4n + 3$ จะได้ว่า

1. ถ้า $3m + n$ เป็นจำนวนเต็มคู่ แล้ว $3p_1p_2 \equiv 1 \pmod{8}$
2. ถ้า $3m + n$ เป็นจำนวนเต็มคี่ แล้ว $-p_1p_2 \equiv 1 \pmod{8}$

บทพิสูจน์

1. สมมติ $3m+n$ เป็นจำนวนเต็มคู่ จะมีจำนวนเต็ม l ที่ทำให้ $3m+n=2l$ จะได้ว่า

$$p_1 p_2 = (4m+1)(4n+3) = 16mn + 4(3m+n) + 3 = 16mn + 4(2l) + 3 = 8(2mn+l) + 3$$

เพราะฉะนั้น

$$3p_1 p_2 = 8(6mn+3l) + 9 = 8(6mn+3l) + 8 + 1 = 8(6mn+3l+1) + 1$$

ดังนั้น $3p_1 p_2 \equiv 1 \pmod{8}$

2. สมมติ $3m+n$ เป็นจำนวนเต็มคี่ จะมีจำนวนเต็ม l ที่ทำให้ $3m+n=2l+1$ จะได้ว่า

$$p_1 p_2 = (4m+1)(4n+3) = 16mn + 4(3m+n) + 3 = 16mn + 4(2l+1) + 3 = 8(2mn+l) + 7$$

เพราะฉะนั้น

$$-p_1 p_2 = 8(-2mn-l) - 7 = 8(-2mn-l) - 8 + 1 = 8(-2mn-l-1) + 1$$

ดังนั้น $-p_1 p_2 \equiv 1 \pmod{8}$

□

ทฤษฎีบท 2.7 ให้ p_1, p_2 และ p เป็นจำนวนเฉพาะคี่ ซึ่ง $p \nmid p_1$ และ $p \nmid p_2$ และ

ถ้า $p_1 = 4m+1$ และ $p_2 = 4n+3$ สำหรับบางจำนวนเต็ม m และ n จะได้ว่า

1. ถ้า $3m+n$ เป็นจำนวนเต็มคู่ แล้ว

$$(2p_1p_2 / p) = \begin{cases} 1, & \begin{aligned} p &\equiv 3p_1p_2 + 32n_5 \left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 32n_5 \left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 32n_5 \left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 32n_5 \left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 32n_5 \left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 32n_5 \left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 32n_5 \left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 32n_5 \left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2} \end{aligned} \\ -1, & \begin{aligned} p &\equiv 3p_1p_2 + 32n_5 \left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 32n_5 \left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 32n_5 \left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 32n_5 \left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 32n_5 \left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 32n_5 \left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 32n_5 \left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 32n_5 \left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2} \end{aligned} \end{cases}$$

เมื่อ $S_1 \in \{2, 4, 6, \dots, p_1 - 1\}$, $S_2 \in \{2, 4, 6, \dots, p_2 - 1\}$, $T_1 \in \{1, 3, 5, \dots, p_1 - 2\}$, $T_2 \in \{1, 3, 5, \dots, p_2 - 2\}$, r_1 และ r_2 เป็นรากปฐมนฐานมอดุโล p_1 และ p_2 ตามลำดับ และ n_3, n_4 และ n_5 เป็นจำนวนเต็มที่สุดคัล้อง $4p_2n_3 \equiv 1 \pmod{p_1}$, $4p_1n_4 \equiv 1 \pmod{p_2}$ และ $8n_5 \equiv 1 \pmod{p_1p_2}$ ตามลำดับ

2. ถ้า $3m+n$ เป็นจำนวนเต็มคี่ แล้ว

$$(2p_1p_2/p) = \begin{cases} 1, & \begin{aligned} p &\equiv -p_1p_2 + 32n_5(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 32n_5(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 32n_5(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 32n_5(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 32n_5(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 32n_5(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 32n_5(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 32n_5(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1) \pmod{8p_1p_2} \end{aligned} \\ -1, & \begin{aligned} p &\equiv -p_1p_2 + 32n_5(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 32n_5(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 32n_5(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 32n_5(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 32n_5(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 32n_5(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 32n_5(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 32n_5(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1) \pmod{8p_1p_2} \end{aligned} \end{cases}$$

เมื่อ $S_1 \in \{2, 4, 6, \dots, p_1-1\}$, $S_2 \in \{2, 4, 6, \dots, p_2-1\}$, $T_1 \in \{1, 3, 5, \dots, p_1-2\}$, $T_2 \in \{1, 3, 5, \dots, p_2-2\}$, r_1 และ r_2 เป็นรากปฐมนฐานมอดุโล p_1 และ p_2 ตามลำดับ และ n_3, n_4 และ n_5 เป็นจำนวนเต็มที่สุดคัล้อง $4p_2n_3 \equiv 1 \pmod{p_1}$, $4p_1n_4 \equiv 1 \pmod{p_2}$ และ $8n_5 \equiv 1 \pmod{p_1p_2}$ ตามลำดับ

กรณีที 3 $p_1 \equiv 3 \pmod{4}$ และ $p_2 \equiv 3 \pmod{4}$

ทฤษฎีบท 2.8 ให้ p_1 และ p_2 เป็นจำนวนเฉพาะคี่ทีทำให้มีจำนวนเต็ม m และ n ซึ่งสอดคล้องกับ $p_1 = 4m+3$ และ $p_2 = 4n+3$ จะได้ว่า

1. ถ้า $m+n$ เป็นจำนวนเต็มคี่ แล้ว $p_1p_2 \equiv 1 \pmod{8}$
2. ถ้า $m+n$ เป็นจำนวนเต็มคี่ แล้ว $-3p_1p_2 \equiv 1 \pmod{8}$

บทพิสูจน์

1. สมมติ $m+n$ เป็นจำนวนเต็มคู่ จะมีจำนวนเต็ม l ที่ทำให้ $m+n = 2l$ จะได้ว่า

$$\begin{aligned} p_1p_2 &= (4m+3)(4n+3) = 16mn + 12(m+n) + 9 = 16mn + 12(2l) + 9 + 1 \\ &= 8(2mn + 3l + 1) + 1 \end{aligned}$$

ดังนั้น $p_1p_2 \equiv 1 \pmod{8}$

2. สมมติ $m+n$ เป็นจำนวนเต็มคี่ จะมีจำนวนเต็ม l ที่ทำให้ $m+n = 2l+1$ จะได้ว่า

$$\begin{aligned} p_1p_2 &= (4m+3)(4n+3) = 16mn + 12(m+n) + 9 = 16mn + 12(2l+1) + 9 \\ &= 8(2mn + 3l) + 21 \end{aligned}$$

เพราะฉะนั้น

$$-3p_1p_2 = 8(-6mn - 9l) - 63 = 8(-6mn - 9l) - 64 + 1 = 8(-6mn - 9l - 8) + 1$$

ดังนั้น $-3p_1p_2 \equiv 1 \pmod{8}$

□

ทฤษฎีบท 2.9 ให้ p_1, p_2 และ p เป็นจำนวนเฉพาะคี่ ซึ่ง $p \nmid p_1$ และ $p \nmid p_2$ และ

ถ้า $p_1 = 4m+3$ และ $p_2 = 4n+3$ สำหรับบางจำนวนเต็ม m และ n จะได้ว่า

1. ถ้า $m+n$ เป็นจำนวนเต็มคู่ แล้ว

$$(2p_1p_2 / p) = \begin{cases} 1, & p \equiv p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ & \equiv p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ & \equiv -p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ & \equiv -p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ & \equiv 3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ & \equiv 3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ & \equiv -3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ & \equiv -3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2} \\ -1, & p \equiv p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ & \equiv p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ & \equiv -p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ & \equiv -p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ & \equiv 3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ & \equiv 3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ & \equiv -3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ & \equiv -3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2} \end{cases}$$

เมื่อ $S_1 \in \{2, 4, 6, \dots, p_1 - 1\}$, $S_2 \in \{2, 4, 6, \dots, p_2 - 1\}$, $T_1 \in \{1, 3, 5, \dots, p_1 - 2\}$,

$T_2 \in \{1, 3, 5, \dots, p_2 - 2\}$, r_1 และ r_2 เป็นรากปฐมฐานมอดุโล p_1 และ p_2 ตามลำดับ และ

n_3, n_4 และ n_5 เป็นจำนวนเต็มที่สอดคล้อง $4p_2n_3 \equiv 1 \pmod{p_1}$, $4p_1n_4 \equiv 1 \pmod{p_2}$

และ $8n_5 \equiv 1 \pmod{p_1p_2}$ ตามลำดับ

2. ถ้า $m+n$ เป็นจำนวนเต็มคี่ แล้ว

$$(2p_1p_2 / p) = \begin{cases} 1, & \begin{aligned} p &\equiv -3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2} \end{aligned} \\ -1, & \begin{aligned} p &\equiv -3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 128n_5 \left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1 \right) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 128n_5 \left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1 \right) \pmod{8p_1p_2} \end{aligned} \end{cases}$$

เมื่อ $S_1 \in \{2, 4, 6, \dots, p_1 - 1\}$, $S_2 \in \{2, 4, 6, \dots, p_2 - 1\}$, $T_1 \in \{1, 3, 5, \dots, p_1 - 2\}$,

$T_2 \in \{1, 3, 5, \dots, p_2 - 2\}$, r_1 และ r_2 เป็นรากปฐมฐานมอดุโล p_1 และ p_2 ตามลำดับ และ n_3, n_4 และ n_5 เป็นจำนวนเต็มที่สอดคล้อง $4p_2n_3 \equiv 1 \pmod{p_1}$, $4p_1n_4 \equiv 1 \pmod{p_2}$ และ $8n_5 \equiv 1 \pmod{p_1p_2}$ ตามลำดับ

การพิสูจน์ทฤษฎีบท 2.5, ทฤษฎีบท 2.7 และทฤษฎีบท 2.8 มีความคล้ายคลึงกันโดยจะใช้ทฤษฎีบท 2.3 เพื่อแบ่งเป็นกรณีย่อย ๆ และใช้ทฤษฎีบท 2.1 และ ทฤษฎีบท 2.2 ในการพิจารณาผลเฉลยของระบบสมการนั้น ๆ ซึ่งในที่นี้ เราจะยกตัวอย่างบทพิสูจน์ของทฤษฎีบท 2.5 กรณีที่ $m+n$ เป็นจำนวนเต็มคู่ อย่างคร่าว ๆ เพื่อให้เห็นแนวทางการพิสูจน์ทฤษฎีบททั้ง 3 ทฤษฎีบท

บทพิสูจน์ทฤษฎีบท 2.5

บทพิสูจน์ จากทฤษฎีบท 1.3 เราทราบว่า

$$(p_1 p_2 / p) = \begin{cases} 1, & p \equiv p_1 p_2 + 2(n_1 r_1^{S_1} p_2 + n_2 r_2^{S_2} p_1) \pmod{2p_1 p_2}, \\ & \equiv p_1 p_2 + 2(n_1 r_1^{T_1} p_2 + n_2 r_2^{T_2} p_1) \pmod{2p_1 p_2} \\ -1, & p \equiv p_1 p_2 + 2(n_1 r_1^{S_1} p_2 + n_2 r_2^{T_2} p_1) \pmod{2p_1 p_2}, \\ & \equiv p_1 p_2 + 2(n_1 r_1^{T_1} p_2 + n_2 r_2^{S_2} p_1) \pmod{2p_1 p_2} \end{cases}$$

เมื่อ $S_1 \in \{2, 4, 6, \dots, p_1 - 1\}$, $S_2 \in \{2, 4, 6, \dots, p_2 - 1\}$, $T_1 \in \{1, 3, 5, \dots, p_1 - 2\}$, $T_2 \in \{1, 3, 5, \dots, p_2 - 2\}$, r_1 และ r_2 เป็นรากปฐมนฐานมอดุโล p_1 และ p_2 ตามลำดับ และ n_1 และ n_2 เป็นจำนวนเต็มสอดคล้องกับ $2p_2 n_1 \equiv 1 \pmod{p_1}$ และ $2p_1 n_2 \equiv 1 \pmod{p_2}$ ตามลำดับ

$$\text{และจาก } (2/p) = \begin{cases} 1, & p \equiv \pm 1 \pmod{8} \\ -1, & p \equiv \pm 3 \pmod{8} \end{cases}$$

สมมติ $m+n$ เป็นจำนวนเต็มคู่ จะได้ว่า

กรณีที่ 1 พิจารณา $(2p_1 p_2 / p) = 1$ จากทฤษฎีบท 2.3 จะได้ว่า $(2/p)(p_1 p_2 / p) = 1$

กรณีที่ 1.1 $(2/p) = 1$ และ $(p_1 p_2 / p) = 1$

กรณีที่ 1.1.1 $p \equiv 1 \pmod{8}$ และ

$$p \equiv p_1 p_2 + 2(n_1 r_1^{S_1} p_2 + n_2 r_2^{S_2} p_1) \pmod{2p_1 p_2}$$

$$\text{จะได้ว่า } p \equiv 1 \pmod{8} \text{ และ } p \equiv p_1 p_2 + 2(n_1 r_1^{S_1} p_2 + n_2 r_2^{S_2} p_1) \pmod{p_1 p_2}$$

$$m_1 = 8$$

$$m'_1 = p_1 p_2$$

$$a_1 = 1$$

$$m_2 = p_1 p_2$$

$$m'_2 = 8$$

$$a_2 = 2(n_1 r_1^{S_1} p_2 + n_2 r_2^{S_2} p_1)$$

$$p_1 p_2 y_1 \equiv 1 \pmod{8} \quad 8y_2 \equiv 1 \pmod{p_1 p_2}$$

จากทฤษฎีบท 2.4 และสมมติฐาน จะได้ว่า $y_1 = 1$ และ $y_2 = n_3$ ตามลำดับ

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1 m'_1 y_1 + a_2 m'_2 y_2 &= (1)(p_1 p_2)(1) + (2(n_1 r_1^{S_1} p_2 + n_2 r_2^{S_2} p_1))(8)(n_3) \\ &= p_1 p_2 + 16n_3(n_1 r_1^{S_1} p_2 + n_2 r_2^{S_2} p_1) \end{aligned}$$

$$\text{ดังนั้น } p \equiv p_1 p_2 + 16n_3(n_1 r_1^{S_1} p_2 + n_2 r_2^{S_2} p_1) \pmod{8p_1 p_2}$$

$$\text{เมื่อ } n_3 \text{ เป็นจำนวนเต็มที่ทำให้ } 8n_3 \equiv 1 \pmod{p_1 p_2}$$

กรณีที่ 1.1.2 $p \equiv 1 \pmod{8}$ และ $p \equiv p_1p_2 + 2(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{2p_1p_2}$

ดังนั้น $p \equiv p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}$

กรณีที่ 1.1.3 $p \equiv -1 \pmod{8}$ และ

$p \equiv p_1p_2 + 2(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{2p_1p_2}$

ดังนั้น $p \equiv -p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}$

กรณีที่ 1.1.4 $p \equiv -1 \pmod{8}$ และ

$p \equiv p_1p_2 + 2(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{2p_1p_2}$

ดังนั้น $p \equiv -p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}$

กรณีที่ 1.2 $(2/p) = -1$ และ $(p_1p_2/p) = -1$

กรณีที่ 1.2.1 $p \equiv 3 \pmod{8}$ และ

$p \equiv p_1p_2 + 2(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{2p_1p_2}$

ดังนั้น $p \equiv 3p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}$

กรณีที่ 1.2.2 $p \equiv 3 \pmod{8}$ และ

$p \equiv p_1p_2 + 2(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{2p_1p_2}$

ดังนั้น $p \equiv 3p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}$

กรณีที่ 1.2.3 $p \equiv -3 \pmod{8}$ และ

$p \equiv p_1p_2 + 2(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{2p_1p_2}$

ดังนั้น $p \equiv -3p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}$

กรณีที่ 1.2.4 $p \equiv -3 \pmod{8}$ และ

$p \equiv p_1p_2 + 2(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{2p_1p_2}$

ดังนั้น $p \equiv -3p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}$

กรณีที่ 2 พิจารณา $(2p_1p_2/p) = -1$ จากทฤษฎีบท 2.3 จะได้ว่า $(2/p)(p_1p_2/p) = -1$

กรณีที่ 2.1 $(2/p) = 1$ และ $(p_1p_2/p) = -1$

กรณีที่ 2.1.1 $p \equiv 1 \pmod{8}$ และ

$p \equiv p_1p_2 + 2(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{2p_1p_2}$

ดังนั้น $p \equiv p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}$

กรณีที่ 2.1.2 $p \equiv 1 \pmod{8}$ และ $p \equiv p_1 p_2 + 2(n_1 r_1^{T_1} p_2 + n_2 r_2^{S_2} p_1) \pmod{2p_1 p_2}$

$$\text{ดังนั้น } p \equiv p_1 p_2 + 16n_3(n_1 r_1^{T_1} p_2 + n_2 r_2^{S_2} p_1) \pmod{8p_1 p_2}$$

กรณีที่ 2.1.3 $p \equiv -1 \pmod{8}$ และ

$$p \equiv p_1 p_2 + 2(n_1 r_1^{S_1} p_2 + n_2 r_2^{T_2} p_1) \pmod{2p_1 p_2}$$

$$\text{ดังนั้น } p \equiv -p_1 p_2 + 16n_3(n_1 r_1^{S_1} p_2 + n_2 r_2^{T_2} p_1) \pmod{8p_1 p_2}$$

กรณีที่ 2.1.4 $p \equiv -1 \pmod{8}$ และ

$$p \equiv p_1 p_2 + 2(n_1 r_1^{T_1} p_2 + n_2 r_2^{S_2} p_1) \pmod{2p_1 p_2}$$

$$\text{ดังนั้น } p \equiv -p_1 p_2 + 16n_3(n_1 r_1^{T_1} p_2 + n_2 r_2^{S_2} p_1) \pmod{8p_1 p_2}$$

กรณีที่ 2.2 $(2/p) = -1$ และ $(p_1 p_2 / p) = 1$

กรณีที่ 2.2.1 $p \equiv 3 \pmod{8}$ และ

$$p \equiv p_1 p_2 + 2(n_1 r_1^{S_1} p_2 + n_2 r_2^{S_2} p_1) \pmod{2p_1 p_2}$$

$$\text{ดังนั้น } p \equiv 3p_1 p_2 + 16n_3(n_1 r_1^{S_1} p_2 + n_2 r_2^{S_2} p_1) \pmod{8p_1 p_2}$$

กรณีที่ 2.2.2 $p \equiv 3 \pmod{8}$ และ

$$p \equiv p_1 p_2 + 2(n_1 r_1^{T_1} p_2 + n_2 r_2^{T_2} p_1) \pmod{2p_1 p_2}$$

$$\text{ดังนั้น } p \equiv 3p_1 p_2 + 16n_3(n_1 r_1^{T_1} p_2 + n_2 r_2^{T_2} p_1) \pmod{8p_1 p_2}$$

กรณีที่ 2.2.3 $p \equiv -3 \pmod{8}$ และ

$$p \equiv p_1 p_2 + 2(n_1 r_1^{S_1} p_2 + n_2 r_2^{S_2} p_1) \pmod{2p_1 p_2}$$

$$\text{ดังนั้น } p \equiv -3p_1 p_2 + 16n_3(n_1 r_1^{S_1} p_2 + n_2 r_2^{S_2} p_1) \pmod{8p_1 p_2}$$

กรณีที่ 2.2.4 $p \equiv -3 \pmod{8}$ และ

$$p \equiv p_1 p_2 + 2(n_1 r_1^{T_1} p_2 + n_2 r_2^{T_2} p_1) \pmod{2p_1 p_2}$$

$$\text{ดังนั้น } p \equiv -3p_1 p_2 + 16n_3(n_1 r_1^{T_1} p_2 + n_2 r_2^{T_2} p_1) \pmod{8p_1 p_2}$$

ดังนั้น

$$(2p_1p_2 / p) = \begin{cases} 1, & \begin{aligned} p &\equiv p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2} \end{aligned} \\ -1, & \begin{aligned} p &\equiv p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv 3p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 16n_3(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1) \pmod{8p_1p_2}, \\ &\equiv -3p_1p_2 + 16n_3(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1) \pmod{8p_1p_2} \end{aligned} \end{cases}$$

เมื่อ $S_1 \in \{2, 4, 6, \dots, p_1 - 1\}$, $S_2 \in \{2, 4, 6, \dots, p_2 - 1\}$, $T_1 \in \{1, 3, 5, \dots, p_1 - 2\}$, $T_2 \in \{1, 3, 5, \dots, p_2 - 2\}$, r_1 และ r_2 เป็นรากปฐมฐานมอดุโล p_1 และ p_2 ตามลำดับ และ n_1, n_2 และ n_3 เป็นจำนวนเต็มสอดคล้องกับ $2p_2n_1 \equiv 1 \pmod{p_1}$, $2p_1n_2 \equiv 1 \pmod{p_2}$ และ $8n_3 \equiv 1 \pmod{p_1p_2}$ ตามลำดับ $\square$

สำหรับกรณี $m+n$ เป็นจำนวนเต็มคู่ เราทำการพิสูจน์ในทำนองเดียวกับการพิสูจน์กรณี $m+n$ เป็นจำนวนเต็มคี่

3. สรุป

การวิจัยครั้งนี้เป็นการศึกษาหารูปแบบของจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ $(2p_1p_2/p)$ เมื่อ p_1, p_2 เป็นจำนวนเฉพาะคี่, $p \nmid p_1$ และ $p \nmid p_2$ โดยแบ่งการพิจารณาออกเป็น 3 กรณี คือ

1. $p_1 \equiv 1 \pmod{4}$ และ $p_2 \equiv 1 \pmod{4}$,
2. $p_1 \equiv 1 \pmod{4}$ และ $p_2 \equiv 3 \pmod{4}$ และ
3. $p_1 \equiv 3 \pmod{4}$ และ $p_2 \equiv 3 \pmod{4}$

และในแต่ละกรณีได้แบ่งเป็น 2 กรณีย่อย โดยได้ใช้ทฤษฎีบทเศษเหลือของจีนซึ่งเป็นทฤษฎีบทพื้นฐานในทางทฤษฎีจำนวนในการคำนวณเพื่อทำให้สามารถหารูปแบบของจำนวนเฉพาะคี่ที่สอดคล้องกับสัญลักษณ์เลอจองด์ได้ และยิ่งไปกว่านั้น ผู้วิจัยคาดหวังว่างานวิจัยนี้อาจจะนำไปสู่การหารูปแบบของจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ใด ๆ ต่อไปในอนาคต

เอกสารอ้างอิง

- [1] อัจฉรา หาญชูวงศ์. (2542). *ทฤษฎีจำนวน*. กรุงเทพมหานคร: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.
- Harnchoowong, A. (1999). *Theory of Numbers*. Bangkok: Chulalongkorn University Printery.
- [2] อภิรัฐ ศิริวรกุล. (2547). จำนวนเฉพาะ p ที่ทำให้ $\det(\text{adj } X) = b$ มีผลเฉลยใน $M_3(\mathbb{Z}_p)$. (โครงการระดับปริญญาตรี, จุฬาลงกรณ์มหาวิทยาลัย).
- Siraworakun, A. (2004). Prime p admitting a solution of $\det(\text{adj } X) = b$ in $M_3(\mathbb{Z}_p)$. (Senior Project, Chulalongkorn University).
- [3] อภิรัฐ ศิริวรกุล, จันทนา วรรณพันธุ์ และ นภลัย สีสด. (2559). รูปแบบจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ (p_1p_2/p) . รายงานการประชุมวิชาการระดับชาติมหาวิทยาลัยราชภัฏกลุ่มศรีอยุธยาครั้งที่ 7. หน้า 759 - 764.
- Siraworakun, A., Wannaphan, C. and Seesod, N. (2016). Forms of Odd Prime Numbers p in Legendre Symbol (p_1p_2/p) . Proceeding of 7th National Conference of Sri-Ayutthaya Rajabhat University Group. p. 759 - 764.