รายงานการวิจัย

รูปแบบจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ $(2p_1p_2/p)$

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

อภิรัฐ ศิระวรกุล

ได้รับทุนอุดหนุนการวิจัยจากมหาวิทยาลัยราชภัฏเทพสตรี
ประจำปีงบประมาณ พ.ศ.2560

มหาวิทยาลัยราชภัฏเทพสตรี

หัวข้อวิจัย รูปแบบจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ $(2p_1p_2 / p)$
ชื่อผู้วิจัย อภิรัฐ ศิระวรกุล
คณะ วิทยาศาสตร์และเทคโนโลยี
ปีการศึกษา 2560

บทคัดย่อ

ในงานวิจัยนี้ เราได้ศึกษารูปแบบจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ $(2p_1p_2 / p)$ เมื่อ p_1, p_2 เป็นจำนวนเฉพาะคี่, $p \nmid p_1$ และ $p \nmid p_2$ โดยใช้ทฤษฎีบทเศษเหลือของจีนในการหาผลเฉลยของระบบสมภาค 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 $p_2 \equiv 3 \pmod 4$

มหาวิทยาลัยราชภัฏเทพสตรี

Research Title	Form of Odd Prime Numbers p in Legendre Symbol $(2p_1p_2 / p)$
Researcher	Apirat Siraworakun
Faculty	Science and Technology
Academic Year	2017

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 $p_2 \equiv 3 \pmod 4$

มหาวิทยาลัยราชภัฏเพชรบุรี

กิตติกรรมประกาศ

งานวิจัยชิ้นนี้เป็นงานวิจัยที่ต่อยอดมาจากโครงงานระดับปริญญาตรีของผู้วิจัยที่ได้รับการปรึกษาเป็นอย่างดีจาก ผศ.ดร.ศจี เพียรสกุล และงานวิจัยเรื่องรูปแบบของจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ (p_1p_2 / p) ที่ผู้วิจัยได้วิจัยร่วมกับ นางสาวจันทนา วรรณพันธุ์ และนางสาวนภาลัย สีสด อีกทั้งงานวิจัยชิ้นนี้ยังได้รับทุนสนับสนุนจากสถาบันวิจัยและพัฒนามหาวิทยาลัยราชภัฏเทพสตรี ฉะนั้นผู้วิจัยขอขอบคุณสถาบันวิจัยและพัฒนามหาวิทยาลัยราชภัฏเทพสตรี สำหรับทุนเพื่อใช้ในการทำงานวิจัยชิ้นนี้ รวมถึง ผศ.ดร.ศจี เพียรสกุล นางสาวจันทนา วรรณพันธุ์ และนางสาวนภาลัย สีสด บุคคลที่มีส่วนเกี่ยวข้องกับงานวิจัยชิ้นนี้ และที่สำคัญที่สุดขอขอบคุณ นางสาวเพ็ญศิริ คงสิทธิ์ ที่เป็นกำลังใจและแรงผลักดันให้มาทำวิจัยชิ้นนี้ได้สำเร็จและสมบูรณ์

อภิรัฐ ศิระวรกุล
ผู้รับผิดชอบโครงการ

มหาวิทยาลัยราชภัฏเทพสตรี

สารบัญ

มหาวิทยาลัยราชภัฏเทพสตรี

บทที่ 1

บทนำ

1.1 ที่มาและความสำคัญของปัญหา

จากโครงงานระดับปริญญาตรีของผู้วิจัย ได้มีการศึกษาหารูปแบบของจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ (b/p) และ $(2b/p)$ เมื่อ b เป็นจำนวนเฉพาะคี่ ที่ $p \nmid b$ และได้ให้ข้อเสนอแนะในการทำงานนี้ต่อ โดยพิจารณาหารูปแบบของจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ (p_1p_2/p) และ $(2p_1p_2/p)$ เมื่อ p_1 และ p_2 เป็นจำนวนเฉพาะคี่ซึ่ง $p \nmid p_1$ และ $p \nmid p_2$ สำหรับการหารูปแบบของจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ (p_1p_2/p) เมื่อ p_1 และ p_2 เป็นจำนวนเฉพาะคี่ซึ่ง $p \nmid p_1$ และ $p \nmid p_2$ ผู้วิจัยได้ร่วมงานกับ นางสาวจันทนา วรรณพันธุ์ และนางสาวนภาลัย สีสด สามารถหารูปแบบในกรณีนี้ได้เสร็จสมบูรณ์แล้ว

ดังนั้นในงานวิจัยนี้ ผู้วิจัยจึงมีแนวความคิดพัฒนางานนี้ต่อตามแนวทางที่โครงงานได้ให้ข้อเสนอแนะไว้ นั่นคือ ผู้วิจัยจะศึกษาหารูปแบบของจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ $(2p_1p_2/p)$ เมื่อ p_1 และ p_2 เป็นจำนวนเฉพาะคี่ซึ่ง $p \nmid p_1$ และ $p \nmid p_2$

1.2 วัตถุประสงค์ของงานวิจัย

ศึกษารูปแบบจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ $(2p_1p_2/p)$ เมื่อ p_1, p_2 เป็นจำนวนเฉพาะคี่, $p \nmid p_1$ และ $p \nmid p_2$

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1.3.1 เพื่อเป็นผลงานวิจัยเพื่อพัฒนาองค์ความรู้ใหม่ของสาขาวิชาคณิตศาสตร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏเทพสตรี

1.3.2 เพื่อเป็นความรู้พื้นฐานในการศึกษาหารูปแบบในกรณีทั่วไป

1.4 ขอบเขตงานวิจัย

ศึกษารูปแบบจำนวนเฉพาะคี่ ที่สอดคล้องกับสัญลักษณ์เลอจองด์ $(2p_1p_2/p)$ เท่านั้น

มหาวิทยาลัยราชภัฏเทพสตรี

1.5 ระยะเวลาของการดำเนินวิจัย

การดำเนินงานวิจัย	ระยะเวลา											
	ต.ค. 59	พ.ย. 59	ธ.ค. 59	ม.ค. 60	ก.พ. 60	มี.ค. 60	เม.ย. 60	พ.ค. 60	มิ.ย. 60	ก.ค. 60	ส.ค. 60	ก.ย. 60
1. ศึกษาความรู้พื้นฐานที่ใช้ในงานวิจัย	←	→										
2. ศึกษาวิธีพิสูจน์จากงานวิจัยที่เกี่ยวข้องเพื่อเป็นพื้นฐานแนวคิดในการทำงานวิจัยชิ้นนี้			←	→								
3. หารูปแบบรูปแบบจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ $(2p_1p_2/p)$ เมื่อ p_1, p_2 เป็นจำนวนเฉพาะคี่, $p \mid p_1$ และ $p \mid p_2$					←			→				
4. สรุปผลการศึกษาวิจัยเพื่อเตรียมการสู่การเผยแพร่ผลการวิจัย									←	→		
5. นำเสนอผลงานวิจัยในงานประชุมวิชาการหรือเผยแพร่ตีพิมพ์ในรูปบทความในวารสารทางวิชาการ											←	→

1.6 สถานที่ดำเนินการวิจัย

สาขาวิชาคณิตศาสตร์ คณะวิทยาศาสตร์และเทคโนโลยี

มหาวิทยาลัยราชภัฏเทพสตรี

บทที่ 2

เอกสารและงานวิจัยที่เกี่ยวข้อง

2.1 นิยามและทฤษฎีบทที่เกี่ยวข้อง

เริ่มต้นเราจะทบทวนนิยามพื้นฐานที่เกี่ยวข้องกับงานวิจัยนี้

บทนิยาม 2.1.1 [1] ให้ a, b เป็นจำนวนเต็ม และ n เป็นจำนวนเต็มบวก เราจะกล่าวว่า a สมภาค หรือ คอนกรูเอนซ์ (Congruence) กับ b มอดุโล n เขียนแทนด้วย $a \equiv b \pmod{n}$ ก็ต่อเมื่อ n หาร $a-b$ ลงตัว

บทนิยาม 2.1.2 [1] กำหนดให้ n เป็นจำนวนเต็มบวก จะได้ว่า $\phi(n)$ เป็นจำนวนของจำนวนเต็มบวกทั้งหมดที่น้อยกว่าหรือ เท่ากับ n และ เป็นจำนวนเฉพาะสัมพัทธ์กับ n

บทนิยาม 2.1.3 [1] กำหนดให้ a และ m เป็นจำนวนเต็มบวกที่ $(a,m)=1$ จะได้ว่า

a เป็นรากปฐมฐาน มอดุโล m ก็ต่อเมื่อ $\phi(m)$ เป็นจำนวนนับที่น้อยที่สุดที่ทำให้ $a^{\phi(m)} \equiv 1 \pmod{m}$

บทนิยาม 2.1.4 [1] กำหนดให้ m เป็นจำนวนเต็มบวก และ a เป็นจำนวนเต็มที่ $(a,m)=1$ เราจะกล่าวว่า a เป็นส่วนตกค้างกำลังสองมอดุโล m เมื่อ $x^2 \equiv a \pmod{m}$ มีผลเฉลย

แต่ถ้า $x^2 \equiv a \pmod{m}$ ไม่มีผลเฉลย เราจะกล่าวว่า a ไม่เป็นส่วนตกค้างกำลังสอง มอดุโล m

บทนิยาม 2.1.5 [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

นอกจากนิยามที่ได้กล่าวข้างต้นแล้ว ยังมีทฤษฎีบทพื้นฐานสำคัญสำหรับงานวิจัยชิ้นนี้คือ ขั้นตอนวิธีการหาร และทฤษฎีบทที่เกี่ยวข้องกับสัญลักษณ์เลอจองด์ ดังต่อไปนี้

มหาวิทยาลัยราชภัฏเทพสตรี

ทฤษฎีบท 2.1.6 [1] **ขั้นตอนวิธีการหาร (The division algorithm)**

ให้ a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$ จะได้ว่า มีจำนวนเต็ม q และ r เพียงคู่เดียวเท่านั้น ซึ่งทำให้

$$b = aq + r \text{ โดยที่ } 0 \leq r < |a|$$

จะเรียก q ว่า ผลหาร (Quotient) และ r ว่า เศษ (Remainder)

ทฤษฎีบท 2.1.7 [1] กำหนดให้ p เป็นจำนวนเฉพาะคี่ และ a, b เป็นจำนวนเต็มที่ $p \nmid a$ และ $p \nmid b$ จะได้ว่า

1. ถ้า $a \equiv b \pmod{p}$ แล้ว $(a/p) = (b/p)$
2. $(ab/p) = (a/p)(b/p)$
3. $(a^2/p) = 1$

ทฤษฎีบท 2.1.8 [1] สำหรับจำนวนเฉพาะคี่ p จะได้ว่า $(2/p) = \begin{cases} 1, & p \equiv \pm 1 \pmod{8} \\ -1, & p \equiv \pm 3 \pmod{8} \end{cases}$

ทฤษฎีบทต่อไปนี้ถือว่ามีความสำคัญเป็นอย่างมากกับงานวิจัยชิ้นนี้ กล่าวคือเป็นทฤษฎีที่ใช้ในการหาผลเฉลยของระบบสมภาคที่นำไปสู่รูปแบบของสัญลักษณ์เลอจองด์ $(2p_1p_2/p)$ เมื่อ p_1, p_2 เป็นจำนวนเฉพาะคี่, $p \nmid p_1$ และ $p \nmid p_2$

ทฤษฎีบท 2.1.9 [1] **ทฤษฎีบทเศษเหลือของจีน (Chinese Remainder Theorem)**

กำหนดให้ $m_1, m_2, m_3, \ldots, m_n$ เป็นจำนวนเต็มบวกที่เป็นจำนวนเฉพาะสัมพัทธ์ทุกคู่ จะได้ว่า ไม่ว่า $a_1, a_2, a_3, \ldots, a_n$ เป็นจำนวนเต็มใดๆ ระบบสมภาค

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\cdots$$
$$x \equiv a_n \pmod{m_n}$$

จะมีผลเฉลยเพียงตัวเดียวมอดุโล m เมื่อ $m = m_1m_2m_3 \ldots m_n$ นั่นคือ มี x_0 เป็นผลเฉลย และผลเฉลยทั้งหมดจะอยู่ในรูป $x_0 + km$ เมื่อ k เป็นจำนวนเต็มใดๆ

มหาวิทยาลัยราชภัฏเทพสตรี

ทฤษฎีบทเศษเหลือของจีนสามารถขยายได้เป็นทฤษฎีที่อธิบายถึงการมีคำตอบของระบบสมภาคเมื่อ $m_1, m_2, m_3, \ldots, m_n$ เป็นจำนวนเต็มบวกใดๆ

ทฤษฎีบท 2.1.10 [1] กำหนดให้ $m_1, m_2, m_3, \ldots, m_n$ เป็นจำนวนเต็มบวก และ $b_1, b_2, b_3, \ldots, b_n$ ที่เป็นจำนวนเต็มใดๆ ระบบสมภาค

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

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

$$\cdots$$

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

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

2.2 งานวิจัยที่เกี่ยวข้อง

อภิรัฐ ศิระวรกุล และคณะ (2559) ได้ศึกษารูปแบบจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ (p_1p_2 / p) เมื่อ p_1 และ p_2 เป็นจำนวนเฉพาะคี่ซึ่ง $p \nmid p_1$ และ $p \nmid p_2$

อภิรัฐ ศิระวรกุล และศจี เพียรสกุล (2547) การศึกษาหารูปแบบของจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ (b / p) และ $(2b / p)$ เมื่อ b เป็นจำนวนเฉพาะคี่ ที่ $p \nmid b$

เพื่อให้เห็นความเชื่อมโยงที่ชัดเจน จึงได้สรุปผลการวิจัยที่เกี่ยวข้องกับการหารูปแบบของจำนวนเฉพาะในสัญลักษณ์เลอจองด์ดังต่อไปนี้

จากการศึกษาโครงงานระดับปริญญาตรี[2] พบว่าได้มีการศึกษารูปแบบจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ (b / p) เมื่อ b เป็นจำนวนเฉพาะที่ $p \nmid b$ มีรายละเอียดดังทฤษฎีดังต่อไปนี้

ทฤษฎีบท 2.2.1 [2] กำหนดให้ b และ p เป็นจำนวนเฉพาะคี่ 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 $S_1 \in \{2, 4, 6, \ldots, b-1\}$ $T_1 \in \{1, 3, 5, \ldots, b-2\}$ และ r เป็นรากปฐมฐาน มอดุโล b

มหาวิทยาลัยราชภัฏเทพสตรี

ทฤษฎีบท 2.2.2 [2] กำหนดให้ b และ p เป็นจำนวนเฉพาะคี่ โดยที่ $p \nmid b$ และ $b \equiv 3 \pmod 4$ จะได้ว่า

$$(b/p) = \begin{cases} 1, & p \equiv 3b + 4n_0 r^{S_1},\ -3b + 4n_0 r^{T_1} \pmod{4b} \\ -1, & p \equiv 3b + 4n_0 r^{T_1},\ -3b + 4n_0 r^{S_1} \pmod{4b} \end{cases}$$

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

และจากงานวิจัยของผู้วิจัย ร่วมกับ นางสาวจันทนา วรรณพันธุ์ และนางสาวนภาลัย สีสด ได้มีการศึกษารูปแบบจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ $(p_1 p_2 / p)$ เมื่อ p_1, p_2 เป็นจำนวนเฉพาะคี่, $p \nmid p_1$ และ $p \nmid p_2$ มีรายละเอียดดังทฤษฎีดังต่อไปนี้

ทฤษฎีบท 2.2.3 [3] กำหนดให้ p_1, p_2 และ p เป็นจำนวนเฉพาะคี่ ซึ่ง $p_1 \equiv 1 \pmod 4$, $p_2 \equiv 1 \pmod 4$, $p \nmid p_1$ และ $p \nmid p_2$ จะได้ว่า

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

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

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

มหาวิทยาลัยราชภัฏเทพสตรี

ทฤษฎีบท 2.2.4 [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

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

เมื่อ $S_1 \in \{2, 4, 6, \ldots, p_1 - 1\}$, $S_2 \in \{2, 4, 6, \ldots, p_2 - 1\}$, $T_1 \in \{1, 3, 5, \ldots, p_1 - 2\}$, $T_2 \in \{1, 3, 5, \ldots, p_2 - 2\}$, 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 2.2.5 [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

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

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

มหาวิทยาลัยราชภัฏเพชรบุรี

$T_2 \in \{1, 3, 5, \ldots, p_2 - 2\}$, r_1 และ r_2 เป็นรากปฐมฐานมอดุโล p_1 และ p_2 ตามลำดับ และ n_0, m_0, n_3 และ n_4 เป็นจำนวนเต็มที่สอดคล้อง

$p_1 = 4n_0 - 1$, $p_2 = 4m_0 - 1$, $4p_2n_3 \equiv 1 \pmod{p_1}$ และ $4p_1n_4 \equiv 1 \pmod{p_2}$ ตามลำดับ

มหาวิทยาลัยราชภัฏเทพสตรี

บทที่ 3

ผลการวิจัย

3.1 รูปแบบจำนวนเฉพาะคี่ p เมื่อ $p_1 \equiv 1 \pmod 4$ และ $p_2 \equiv 1 \pmod 4$

ทฤษฎีบท 3.1.1 : ให้ p_1 และ p_2 เป็นจำนวนเฉพาะคี่ โดยที่ $p_1 \equiv 1 \pmod 4$ และ $p_2 \equiv 1 \pmod 4$ เพราะฉะนั้นเราสามารถเขียน $p_1 = 4m+1$ และ $p_2 = 4n+1$ สำหรับบางจำนวนเต็ม m และ n

1. ถ้า $m+n$ เป็นจำนวนเต็มคู่ แล้ว $p_1 p_2 \equiv 1 \pmod 8$
2. ถ้า $m+n$ เป็นจำนวนเต็มคี่ แล้ว $-3p_1 p_2 \equiv 1 \pmod 8$

พิสูจน์ : 1. สมมติ $m+n$ เป็นจำนวนเต็มคู่ เราสามารถเขียน $m+n = 2l$ สำหรับบางจำนวนเต็ม l เพราะฉะนั้น

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

ดังนั้น $p_1 p_2 \equiv 1 \pmod 8$

2. สมมติ $m+n$ เป็นจำนวนเต็มคี่ เราสามารถเขียน $m+n = 2l+1$ บางจำนวนเต็ม l จะได้ว่า $p_1 p_2 = (4m+1)(4n+1) = 16mn + 4(m+n) + 1 = 16mn + 4(2l+1) + 1 = 8(2mn+l) + 5$

เพราะฉะนั้น $-3p_1 p_2 = 8(-6mn-3l) - 15 = 8(-6mn-3l) - 16 + 1 = 8(-6mn-3l-2) + 1$

ดังนั้น $-3p_1 p_2 \equiv 1 \pmod 8$

ทฤษฎีบท 3.1.2 : ให้ p_1, p_2 และ p เป็นจำนวนเฉพาะคี่ ซึ่ง $p_1 \equiv 1 \pmod 4$, $p_2 \equiv 1 \pmod 4$, $p \nmid p_1$ และ $p \nmid p_2$ เพราะฉะนั้นเราสามารถเขียน $p_1 = 4m+1$ และ $p_2 = 4n+1$ สำหรับบางจำนวนเต็ม m และ n

มหาวิทยาลัยราชภัฏเทพสตรี

1. ถ้า $m+n$ เป็นจำนวนเต็มคู่ แล้ว

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

เมื่อ $S_1 \in \{2,\ 4,\ 6,\ \ldots,\ p_1-1\}$, $S_2 \in \{2,\ 4,\ 6,\ \ldots,\ p_2-1\}$, $T_1 \in \{1,\ 3,\ 5,\ \ldots,\ p_1-2\}$, $T_2 \in \{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, 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

มหาวิทยาลัยรามคำแหง

2. ถ้า $m+n$ เป็นจำนวนเต็มคี่ แล้ว

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

เมื่อ $S_1 \in \{2, 4, 6, \ldots, p_1 - 1\}$, $S_2 \in \{2, 4, 6, \ldots, p_2 - 1\}$, $T_1 \in \{1, 3, 5, \ldots, p_1 - 2\}$, $T_2 \in \{1, 3, 5, \ldots, p_2 - 2\}$, 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

มหาวิทยาลัยราชภัฏสวนสุนันทา

พิสูจน์ จากทฤษฎีบท เราทราบว่า

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

เมื่อ $S_1\in\{2,\ 4,\ 6,\ \ldots,\ p_1-1\}$, $S_2\in\{2,\ 4,\ 6,\ \ldots,\ p_2-1\}$, $T_1\in\{1,\ 3,\ 5,\ \ldots,\ p_1-2\}$, $T_2\in\{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, 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

และ $(2/p)=\begin{cases}1, & p\equiv\pm1\pmod 8\\ -1, & p\equiv\pm3\pmod 8\end{cases}$

1. สมมติ $m+n$ เป็นจำนวนเต็มคู่ จะได้ว่า

กรณีที่ 1 พิจารณา $(2p_1p_2/p)=1$

จากทฤษฎีบท จะได้ว่า $(2/p)(p_1p_2/p)=1$

กรณีที่ 1.1 $(2/p)=1$ และ $(p_1p_2/p)=1$

กรณีที่ 1.1.1 $p\equiv 1\pmod 8$ และ $p\equiv p_1p_2+2\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right)\pmod{2p_1p_2}$

จะได้ว่า $p\equiv 1\pmod 8$ และ $p\equiv p_1p_2+2\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right)\pmod{p_1p_2}$

$m_1=8$	$m_1'=p_1p_2$	$a_1=1$
$m_2=p_1p_2$	$m_2'=8$	$a_2=2\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right)$
$p_1p_2y_1\equiv 1\pmod 8$	$8y_2\equiv 1\pmod{p_1p_2}$	$y_1=1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned}a_1m_1'y_1+a_2m_2'y_2&=(1)(p_1p_2)(1)+\left(2\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right)\right)(8)(n_3)\\&=p_1p_2+16n_3\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right)\end{aligned}$$

ดังนั้น $p\equiv p_1p_2+16n_3\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right)\pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็มที่ทำให้ $8n_3\equiv 1\pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

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

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

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (1)(p_1p_2)(1) + \left(2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.1.3 $p \equiv -1 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -1 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-1)(p_1p_2)(1) + \left(2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= -p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

กรณีที่ 1.1.4 $p \equiv -1 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -1 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-1)(p_1p_2)(1) + \left(2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= -p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

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

กรณีที่ 1.2.1 $p \equiv 3 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv 3 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (3)(p_1p_2)(1) + \left(2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= 3p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv 3p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเพชรบุรี

กรณีที่ 1.2.2 $p \equiv 3 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv 3 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (3)(p_1p_2)(1) + \left(2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= 3p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv 3p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.3 $p \equiv -3 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -3 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-3)(p_1p_2)(1) + \left(2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= -3p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -3p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

กรณีที่ 1.2.4 $p \equiv -3 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -3 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-3)(p_1p_2)(1) + \left(2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= -3p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -3p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

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

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

จะได้ว่า $p \equiv 1 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (1)(p_1p_2)(1) + \left(2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเพชรบุรี

กรณีที่ 2.1.2 $p \equiv 1 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ $p \equiv 1 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (1)(p_1p_2)(1) + \left(2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.3 $p \equiv -1 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -1 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-1)(p_1p_2)(1) + \left(2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= -p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

กรณีที่ 2.1.4 $p \equiv -1 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -1 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-1)(p_1p_2)(1) + \left(2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= -p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2 $(2/p) = -1$ และ $(p_1p_2/p) = 1$

กรณีที่ 2.2.1 $p \equiv 3 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv 3 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (3)(p_1p_2)(1) + \left(2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= 3p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv 3p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

กรณีที่ 2.2.2 $p \equiv 3 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv 3 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (3)(p_1p_2)(1) + \left(2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= 3p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv 3p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.3 $p \equiv -3 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -3 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-3)(p_1p_2)(1) + \left(2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= -3p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -3p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

กรณีที่ 2.2.4 $p \equiv -3 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -3 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$	$m_1' = p_1p_2$	$a_1 = -3$
$m_2 = p_1p_2$	$m_2' = 8$	$a_2 = 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right)$
$p_1p_2y_1 \equiv 1 \pmod 8$	$8y_2 \equiv 1 \pmod{p_1p_2}$	$y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-3)(p_1p_2)(1) + \left(2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= -3p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -3p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

จากกรณีทั้งหมดเราสรุปได้ว่า

มหาวิทยาลัยราชภัฏเทพสตรี

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

เมื่อ $S_1\in\{2,\ 4,\ 6,\ \ldots,\ p_1-1\}$, $S_2\in\{2,\ 4,\ 6,\ \ldots,\ p_2-1\}$, $T_1\in\{1,\ 3,\ 5,\ \ldots,\ p_1-2\}$, $T_2\in\{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, 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. สมมติ $m+n$ เป็นจำนวนเต็มคี่ จะได้ว่า

กรณีที่ 1 พิจารณา $(2p_1p_2/p)=1$

จากทฤษฎีบท จะได้ว่า $(2/p)(p_1p_2/p)=1$

มหาวิทยาลัยการกีฬาแห่งชาติ

กรณีที่ 1.1 $(2/p)=1$ และ $(p_1p_2/p)=1$

กรณีที่ 1.1.1 $p\equiv 1 \pmod 8$ และ $p\equiv p_1p_2+2\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p\equiv 1 \pmod 8$ และ $p\equiv 2\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=1$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=2\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1\equiv 1 \pmod 8$ $\quad 8y_2\equiv 1 \pmod{p_1p_2}$ $\quad y_1=-3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1+a_2m_2'y_2 &= (1)(p_1p_2)(-3)+\left(2\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= -3p_1p_2+16n_3\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p\equiv -3p_1p_2+16n_3\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็มที่ทำให้ $8n_3\equiv 1 \pmod{p_1p_2}$

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

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

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=1$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=2\left(n_1r_1^{T_1}p_2+n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1\equiv 1 \pmod 8$ $\quad 8y_2\equiv 1 \pmod{p_1p_2}$ $\quad y_1=-3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1+a_2m_2'y_2 &= (1)(p_1p_2)(-3)+\left(2\left(n_1r_1^{T_1}p_2+n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= -3p_1p_2+16n_3\left(n_1r_1^{T_1}p_2+n_2r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p\equiv -3p_1p_2+16n_3\left(n_1r_1^{T_1}p_2+n_2r_2^{T_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็มที่ทำให้ $8n_3\equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเพชรบุรี

กรณีที่ 1.1.3 $p \equiv -1 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -1 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-1)(p_1p_2)(-3) + \left(2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= 3p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv 3p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.1.4 $p \equiv -1 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -1 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-1)(p_1p_2)(-3) + \left(2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= 3p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv 3p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏพิบูลสงคราม

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

กรณีที่ 1.2.1 $p\equiv 3 \pmod 8$ และ $p\equiv p_1p_2+2\left(n_1r_1^{S_1}p_2+n_2r_2^{T_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p\equiv 3 \pmod 8$ และ $p\equiv 2\left(n_1r_1^{S_1}p_2+n_2r_2^{T_2}p_1\right) \pmod{p_1p_2}$

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=3$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=2\left(n_1r_1^{S_1}p_2+n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1\equiv 1 \pmod 8$ $\quad 8y_2\equiv 1 \pmod{p_1p_2}$ $\quad y_1=-3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1+a_2m_2'y_2 &= (3)(p_1p_2)(-3)+\left(2\left(n_1r_1^{S_1}p_2+n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= -9p_1p_2+16n_3\left(n_1r_1^{S_1}p_2+n_2r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p\equiv -p_1p_2+16n_3\left(n_1r_1^{S_1}p_2+n_2r_2^{T_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3\equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.2 $p\equiv 3 \pmod 8$ และ $p\equiv p_1p_2+2\left(n_1r_1^{T_1}p_2+n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p\equiv 3 \pmod 8$ และ $p\equiv 2\left(n_1r_1^{T_1}p_2+n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=3$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=2\left(n_1r_1^{T_1}p_2+n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1\equiv 1 \pmod 8$ $\quad 8y_2\equiv 1 \pmod{p_1p_2}$ $\quad y_1=-3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1+a_2m_2'y_2 &= (3)(p_1p_2)(-3)+\left(2\left(n_1r_1^{T_1}p_2+n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= -9p_1p_2+16n_3\left(n_1r_1^{T_1}p_2+n_2r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p\equiv -p_1p_2+16n_3\left(n_1r_1^{T_1}p_2+n_2r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3\equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏพิบูลสงคราม

กรณีที่ 1.2.3 $p \equiv -3 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -3 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-3)(p_1p_2)(-3) + \left(2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= 9p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \end{aligned}$$

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

ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.4 $p \equiv -3 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -3 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-3)(p_1p_2)(-3) + \left(2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= 9p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \end{aligned}$$

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

ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

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

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

มหาวิทยาลัยราชภัฏเพชรบุรี

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

กรณีที่ 2.1.1 $p\equiv 1 \pmod 8$ และ $p\equiv p_1p_2+2\left(n_1r_1^{S_1}p_2+n_2r_2^{T_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p\equiv 1 \pmod 8$ และ $p\equiv 2\left(n_1r_1^{S_1}p_2+n_2r_2^{T_2}p_1\right) \pmod{p_1p_2}$

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=1$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=2\left(n_1r_1^{S_1}p_2+n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1\equiv 1 \pmod 8$ $\quad 8y_2\equiv 1 \pmod{p_1p_2}$ $\quad y_1=-3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1+a_2m_2'y_2 &= (1)(p_1p_2)(-3)+\left(2\left(n_1r_1^{S_1}p_2+n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= -3p_1p_2+16n_3\left(n_1r_1^{S_1}p_2+n_2r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p\equiv -3p_1p_2+16n_3\left(n_1r_1^{S_1}p_2+n_2r_2^{T_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็มที่ทำให้ $8n_3\equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.2 $p\equiv 1 \pmod 8$ และ $p\equiv p_1p_2+2\left(n_1r_1^{T_1}p_2+n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p\equiv 1 \pmod 8$ และ $p\equiv 2\left(n_1r_1^{T_1}p_2+n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=1$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=2\left(n_1r_1^{T_1}p_2+n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1\equiv 1 \pmod 8$ $\quad 8y_2\equiv 1 \pmod{p_1p_2}$ $\quad y_1=-3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1+a_2m_2'y_2 &= (1)(p_1p_2)(-3)+\left(2\left(n_1r_1^{T_1}p_2+n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= -3p_1p_2+16n_3\left(n_1r_1^{T_1}p_2+n_2r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p\equiv -3p_1p_2+16n_3\left(n_1r_1^{T_1}p_2+n_2r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็มที่ทำให้ $8n_3\equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเพชรบุรี

กรณีที่ 2.1.3 $p \equiv -1 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -1 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-1)(p_1p_2)(-3) + \left(2\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= 3p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv 3p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.4 $p \equiv -1 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -1 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-1)(p_1p_2)(-3) + \left(2\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= 3p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv 3p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏพิบูลสงคราม

กรณีที่ 2.2 $(2/p)=-1$ และ $(p_1p_2/p)=1$

กรณีที่ 2.2.1 $p\equiv 3 \pmod 8$ และ $p\equiv p_1p_2+2\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p\equiv 3 \pmod 8$ และ $p\equiv 2\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=3$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=2\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1\equiv 1 \pmod 8$ $\quad 8y_2\equiv 1 \pmod{p_1p_2}$ $\quad y_1=-3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1+a_2m_2'y_2 &= (3)(p_1p_2)(-3)+\left(2\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= -9p_1p_2+16n_3\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p\equiv -p_1p_2+16n_3\left(n_1r_1^{S_1}p_2+n_2r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3\equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.2 $p\equiv 3 \pmod 8$ และ $p\equiv p_1p_2+2\left(n_1r_1^{T_1}p_2+n_2r_2^{T_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p\equiv 3 \pmod 8$ และ $p\equiv 2\left(n_1r_1^{T_1}p_2+n_2r_2^{T_2}p_1\right) \pmod{p_1p_2}$

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=3$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=2\left(n_1r_1^{T_1}p_2+n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1\equiv 1 \pmod 8$ $\quad 8y_2\equiv 1 \pmod{p_1p_2}$ $\quad y_1=-3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1+a_2m_2'y_2 &= (3)(p_1p_2)(-3)+\left(2\left(n_1r_1^{T_1}p_2+n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= -9p_1p_2+16n_3\left(n_1r_1^{T_1}p_2+n_2r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p\equiv -p_1p_2+16n_3\left(n_1r_1^{T_1}p_2+n_2r_2^{T_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_3 เป็นจำนวนเต็ม ที่ทำให้ $8n_3\equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเพชรบุรี

กรณีที่ 2.2.3 $p \equiv -3 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -3 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-3)(p_1p_2)(-3) + \left(2\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right)\right)(8)(n_3) \\ &= 9p_1p_2 + 16n_3\left(n_1r_1^{S_1}p_2 + n_2r_2^{S_2}p_1\right) \end{aligned}$$

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

ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.4 $p \equiv -3 \pmod 8$ และ $p \equiv p_1p_2 + 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{2p_1p_2}$

จะได้ว่า $p \equiv -3 \pmod 8$ และ $p \equiv 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \pmod{p_1p_2}$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-3)(p_1p_2)(-3) + \left(2\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right)\right)(8)(n_3) \\ &= 9p_1p_2 + 16n_3\left(n_1r_1^{T_1}p_2 + n_2r_2^{T_2}p_1\right) \end{aligned}$$

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

ที่ทำให้ $8n_3 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเพชรบุรี

จากกรณีทั้งหมดเราสรุปได้ว่า

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

เมื่อ $S_1\in\{2,\ 4,\ 6,\ \ldots,\ p_1-1\}$, $S_2\in\{2,\ 4,\ 6,\ \ldots,\ p_2-1\}$, $T_1\in\{1,\ 3,\ 5,\ \ldots,\ p_1-2\}$, $T_2\in\{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, 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

มหาวิทยาลัยราชภัฏเพชรบุรี

3.2 รูปแบบจำนวนเฉพาะคี่ p เมื่อ $p_1 \equiv 1 \pmod 4$ และ $p_2 \equiv 3 \pmod 4$

ทฤษฎีบท 3.2.1 : ให้ p_1 และ p_2 เป็นจำนวนเฉพาะคี่ โดยที่ $p_1 \equiv 1 \pmod 4$ และ $p_2 \equiv 3 \pmod 4$ เพราะฉะนั้นเราสามารถเขียน $p_1 = 4m+1$ และ $p_2 = 4n+3$ สำหรับบางจำนวนเต็ม m และ n

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

พิสูจน์ : 1 สมมติ $3m+n$ เป็นจำนวนเต็มคู่ เราสามารถเขียน $3m+n=2l$ สำหรับบางจำนวนเต็ม l จะได้ว่า

$$p_1p_2 = (4m+1)(4n+3) = 16mn + 4(3m+n) + 3 = 16mn + 4(2l) + 3 = 8(2mn+l) + 3$$

เพราะฉะนั้น $3p_1p_2 = 8(6mn+3l) + 9 = 8(6mn+3l) + 8 + 1 = 8(6mn+3l+1) + 1$

ดังนั้น $3p_1p_2 \equiv 1 \pmod 8$

2. สมมติ $3m+n$ เป็นจำนวนเต็มคี่ เราสามารถเขียน $3m+n = 2l+1$ สำหรับบางจำนวนเต็ม l

จะได้ว่า

$$p_1p_2 = (4m+1)(4n+3) = 16mn + 4(3m+n) + 3 = 16mn + 4(2l+1) + 3 = 8(2mn+l) + 7$$

เพราะฉะนั้น $-p_1p_2 = 8(-2mn-l) - 7 = 8(-2mn-l) - 8 + 1 = 8(-2mn-l-1) + 1$

ดังนั้น $-p_1p_2 \equiv 1 \pmod 8$

ทฤษฎีบท 3.2.2 : ให้ 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 $p \nmid p_2$ เพราะฉะนั้นเราสามารถเขียน $p_1 = 4m+1$ และ $p_2 = 4n+3$ สำหรับบางจำนวนเต็ม m และ n

มหาวิทยาลัยราชภัฏเพชรบุรี

1. ถ้า $3m+n$ เป็นจำนวนเต็มคู่ แล้ว

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

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

$T_2\in\{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, 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

มหาวิทยาลัยรังสิต Rangsit University

2. ถ้า $3m+n$ เป็นจำนวนเต็มคี่ แล้ว

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

เมื่อ $S_1 \in \{2,\ 4,\ 6,\ \ldots,\ p_1-1\}$, $S_2 \in \{2,\ 4,\ 6,\ \ldots,\ p_2-1\}$, $T_1 \in \{1,\ 3,\ 5,\ \ldots,\ p_1-2\}$, $T_2 \in \{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, 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

มหาวิทยาลัยรังสิต Rangsit University

พิสูจน์ จากทฤษฎีบท เราทราบว่า

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

เมื่อ $S_1\in\{2,\ 4,\ 6,\ \ldots,\ p_1-1\}$, $S_2\in\{2,\ 4,\ 6,\ \ldots,\ p_2-1\}$, $T_1\in\{1,\ 3,\ 5,\ \ldots,\ p_1-2\}$, $T_2\in\{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, 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

และ $(2/p)=\begin{cases}1, & p\equiv\pm 1\pmod 8\\ -1, & p\equiv\pm 3\pmod 8\end{cases}$ เพราะฉะนั้น $n_0=n+1$ ส่งผลให้

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

เมื่อ $S_1\in\{2,\ 4,\ 6,\ \ldots,\ p_1-1\}$, $S_2\in\{2,\ 4,\ 6,\ \ldots,\ p_2-1\}$, $T_1\in\{1,\ 3,\ 5,\ \ldots,\ p_1-2\}$, $T_2\in\{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, r_1 และ r_2 เป็นรากปฐมฐานมอดุโล p_1 และ p_2 ตามลำดับ

มหาวิทยาลัยราชภัฏพิบูลสงคราม

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

1. สมมติ $3m+n$ เป็นจำนวนเต็มคู่ จะได้ว่า

กรณีที่ 1 พิจารณา $(2p_1p_2 / p) = 1$

จากทฤษฎีบท จะได้ว่า $(2/p)(p_1p_2/p) = 1$

กรณีที่ 1.1 $(2/p) = 1$ และ $(p_1p_2/p) = 1$

กรณีที่ 1.1.1 $p \equiv -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 1 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (1)(p_1p_2)(3) + \left(4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= 3p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv 3p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.1.2 $p \equiv p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 1 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) - 1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

มหาวิทยาลัยราชภัฏเทพสตรี

กรณีที่ 1.1.3 $p \equiv -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 1 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 1 \pmod 8$

$m_1 = 8$	$m_1' = p_1p_2$	$a_1 = 1$
$m_2 = p_1p_2$	$m_2' = 8$	$a_2 = 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$
$p_1p_2y_1 \equiv 1 \pmod 8$	$8y_2 \equiv 1 \pmod{p_1p_2}$	$y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (1)(p_1p_2)(3) + \left(4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5) \\ &= 3p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv 3p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.1.4 $p \equiv p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 1 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) - 1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.5 $p \equiv -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.6 $p \equiv p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

มหาวิทยาลัยราชภัฏเพชรบุรี

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-1)(p_1p_2)(3) + \left(4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5) \\ &= -3p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -3p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.1.7 $p \equiv -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.8 $p \equiv p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-1)(p_1p_2)(3) + \left(4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5) \\ &= -3p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -3p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

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

กรณีที่ 1.2.1 $p \equiv -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 3 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) - 3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.2.2 $p \equiv p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 3 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (3)(p_1p_2)(3) + \left(4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5) \\ &= 9p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.3 $p \equiv -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 3 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) - 3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

มหาวิทยาลัยราชภัฏเทพสตรี

กรณีที่ 1.2.4 $p \equiv p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 3 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (3)(p_1p_2)(3) + \left(4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= 9p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.5 $p \equiv -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-3)(p_1p_2)(3) + \left(4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= -9p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv -p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏพิบูลสงคราม

กรณีที่ 1.2.6 $p \equiv p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.2.7 $p \equiv -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-3)(p_1p_2)(3) + \left(4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= -9p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv -p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.8 $p \equiv p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

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

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

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

มหาวิทยาลัยราชภัฏพิบูลสงคราม

กรณีที่ 2.1.1 $p \equiv -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 1 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (1)(p_1p_2)(3) + \left(4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= 3p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv 3p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_5 เป็นจำนวนเต็ม

ที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.2 $p \equiv p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 1 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) - 1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.1.3 $p \equiv -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 1 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

มหาวิทยาลัยราชภัฏพิบูลสงคราม

$$a_1m_1'y_1 + a_2m_2'y_2 = (1)(p_1p_2)(3) + \left(4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= 3p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv 3p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.4 $p \equiv p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 1 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) - 1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.1.5 $p \equiv -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.1.6 $p \equiv p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

$m_1 = 8$	$m_1' = p_1p_2$	$a_1 = -1$
$m_2 = p_1p_2$	$m_2' = 8$	$a_2 = 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$
$p_1p_2y_1 \equiv 1 \pmod 8$	$8y_2 \equiv 1 \pmod{p_1p_2}$	$y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-1)(p_1p_2)(3) + \left(4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= -3p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv -3p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.7 $p \equiv -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.1.8 $p \equiv p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-1)(p_1p_2)(3) + \left(4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5) \\ &= -3p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -3p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2 $(2/p) = -1$ และ $(p_1p_2/p) = 1$

กรณีที่ 2.2.1 $p \equiv -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 3 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) - 3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.2.2 $p \equiv p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

มหาวิทยาลัยราชภัฏเพชรบุรี

$p \equiv 3 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3 r_1^{S_1} p_2 + 4(n+1) n_4 r_2^{T_2} p_1\right) \pmod{p_1 p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1 p_2$ $\quad a_1 = 3$

$m_2 = p_1 p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3 r_1^{S_1} p_2 + 4(n+1) n_4 r_2^{T_2} p_1\right)$

$p_1 p_2 y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1 p_2}$ $\quad y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1 m_1' y_1 + a_2 m_2' y_2 &= (3)(p_1 p_2)(3) + \left(4\left(n_3 r_1^{S_1} p_2 + 4(n+1) n_4 r_2^{T_2} p_1\right)\right)(8)(n_5) \\ &= 9 p_1 p_2 + 32 n_5 \left(n_3 r_1^{S_1} p_2 + 4(n+1) n_4 r_2^{T_2} p_1\right) \end{aligned}$$

ดังนั้น $p \equiv p_1 p_2 + 32 n_5 \left(n_3 r_1^{S_1} p_2 + 4(n+1) n_4 r_2^{T_2} p_1\right) \pmod{8 p_1 p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1 p_2}$

กรณีที่ 2.2.3 $p \equiv -p_1 p_2 + 4\left(n_3 r_1^{T_1} p_2 + 4(n+1) n_4 r_2^{T_2} p_1\right) \pmod{4 p_1 p_2}$ และ

$p \equiv 3 \pmod 8$ เนื่องจาก $4 \nmid -p_1 p_2 + 4\left(n_3 r_1^{T_1} p_2 + 4(n+1) n_4 r_2^{T_2} p_1\right) - 3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.2.4 $p \equiv p_1 p_2 + 4\left(n_3 r_1^{T_1} p_2 + 4(n+1) n_4 r_2^{S_2} p_1\right) \pmod{4 p_1 p_2}$ และ

$p \equiv 3 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3 r_1^{T_1} p_2 + 4(n+1) n_4 r_2^{S_2} p_1\right) \pmod{p_1 p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1 p_2$ $\quad a_1 = 3$

$m_2 = p_1 p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3 r_1^{T_1} p_2 + 4(n+1) n_4 r_2^{S_2} p_1\right)$

$p_1 p_2 y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1 p_2}$ $\quad y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1 m_1' y_1 + a_2 m_2' y_2 &= (3)(p_1 p_2)(3) + \left(4\left(n_3 r_1^{T_1} p_2 + 4(n+1) n_4 r_2^{S_2} p_1\right)\right)(8)(n_5) \\ &= 9 p_1 p_2 + 32 n_5 \left(n_3 r_1^{T_1} p_2 + 4(n+1) n_4 r_2^{S_2} p_1\right) \end{aligned}$$

มหาวิทยาลัยราชภัฏเพชรบุรี

ดังนั้น $p \equiv p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.5 $p \equiv -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-3)(p_1p_2)(3) + \left(4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5) \\ &= -9p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.6 $p \equiv p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

มหาวิทยาลัยราชภัฏเพชรบุรี

กรณีที่ 2.2.7 $p \equiv -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-3)(p_1p_2)(3) + \left(4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5) \\ &= -9p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.8 $p \equiv p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

มหาวิทยาลัยราชภัฏเพชรบุรี

จากกรณีทั้งหมดเราสรุปได้ว่า

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

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

$T_2 \in \{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, 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

มหาวิทยาลัยรามคำแหง

2. สมมติ $3m+n$ เป็นจำนวนเต็มคี่ จะได้ว่า

กรณีที่ 1 พิจารณา $(2p_1p_2/p)=1$

จากทฤษฎีบท จะได้ว่า $(2/p)(p_1p_2/p)=1$

กรณีที่ 1.1 $(2/p)=1$ และ $(p_1p_2/p)=1$

กรณีที่ 1.1.1 $p\equiv -p_1p_2+4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 1 \pmod 8$ จะได้ว่า $p\equiv 4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p\equiv 1 \pmod 8$

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=1$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1\equiv 1 \pmod 8$ $\quad 8y_2\equiv 1 \pmod{p_1p_2}$ $\quad y_1=-1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1+a_2m_2'y_2=(1)(p_1p_2)(-1)+\left(4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$=-p_1p_2+32n_5\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p\equiv -p_1p_2+32n_5\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5\equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.1.2 $p\equiv p_1p_2+4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 1 \pmod 8$ เนื่องจาก $4\nmid p_1p_2+4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right)-1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.3 $p\equiv -p_1p_2+4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 1 \pmod 8$ จะได้ว่า $p\equiv 4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p\equiv 1 \pmod 8$

มหาวิทยาลัยราชภัฏพิบูลสงคราม

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (1)(p_1p_2)(-1) + \left(4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5) \\ &= -p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$.

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.1.4 $p \equiv p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 1 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) - 1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.5 $p \equiv -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.6 $p \equiv p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

มหาวิทยาลัยราชภัฏเทพสตรี

$$a_1m_1'y_1 + a_2m_2'y_2 = (-1)(p_1p_2)(-1) + \left(4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.1.7 $p \equiv -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.8 $p \equiv p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

$m_1 = 8$	$m_1' = p_1p_2$	$a_1 = -1$
$m_2 = p_1p_2$	$m_2' = 8$	$a_2 = 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$
$p_1p_2y_1 \equiv 1 \pmod 8$	$8y_2 \equiv 1 \pmod{p_1p_2}$	$y_1 = -1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-1)(p_1p_2)(-1) + \left(4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

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

กรณีที่ 1.2.1 $p\equiv -p_1p_2+4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 3 \pmod 8$ เนื่องจาก $4\nmid -p_1p_2+4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right)-3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.2.2 $p\equiv p_1p_2+4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 3 \pmod 8$ จะได้ว่า $p\equiv 4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p\equiv 3 \pmod 8$

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=3$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1\equiv 1 \pmod 8$ $\quad 8y_2\equiv 1 \pmod{p_1p_2}$ $\quad y_1=-1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1+a_2m_2'y_2=(3)(p_1p_2)(-1)+\left(4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$=-3p_1p_2+32n_5\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p\equiv -3p_1p_2+32n_5\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5\equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.3 $p\equiv -p_1p_2+4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 3 \pmod 8$ เนื่องจาก $4\nmid -p_1p_2+4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right)-3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

มหาวิทยาลัยราชภัฏเทพสตรี

กรณีที่ 1.2.4 $p \equiv p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 3 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (3)(p_1p_2)(-1) + \left(4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5) \\ &= -3p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv -3p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.5 $p \equiv -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-3)(p_1p_2)(-1) + \left(4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5) \\ &= 3p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv 3p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเพชรบุรี

กรณีที่ 1.2.6 $p \equiv p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.2.7 $p \equiv -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ จะได้ $p \equiv 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1 + a_2m_2'y_2 &= (-3)(p_1p_2)(-1) + \left(4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5) \\ &= 3p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p \equiv 3p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.8 $p \equiv p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

มหาวิทยาลัยเชียงใหม่

กรณีที่ 2 พิจารณา $(2p_1p_2/p)=-1$

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

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

กรณีที่ 2.1.1 $p\equiv -p_1p_2+4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 1 \pmod 8$ จะได้ว่า $p\equiv 4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p\equiv 1 \pmod 8$

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=1$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1\equiv 1 \pmod 8$ $\quad 8y_2\equiv 1 \pmod{p_1p_2}$ $\quad y_1=-1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1+a_2m_2'y_2=(1)(p_1p_2)(-1)+\left(4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$=-p_1p_2+32n_5\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p\equiv -p_1p_2+32n_5\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5\equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.2 $p\equiv p_1p_2+4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 1 \pmod 8$ เนื่องจาก $4\nmid p_1p_2+4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right)-1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.1.3 $p\equiv -p_1p_2+4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 1 \pmod 8$ จะได้ว่า $p\equiv 4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p\equiv 1 \pmod 8$

มหาวิทยาลัยรามคำแหง

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (1)(p_1p_2)(-1) + \left(4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= -p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv -p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.4 $p \equiv p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 1 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) - 1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.1.5 $p \equiv -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.1.6 $p \equiv p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

มหาวิทยาลัยราชภัฏเทพสตรี

$$a_1m_1'y_1 + a_2m_2'y_2 = (-1)(p_1p_2)(-1) + \left(4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.7 $p \equiv -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.1.8 $p \equiv p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-1)(p_1p_2)(-1) + \left(4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

กรณีที่ 2.2 $(2/p)=-1$ และ $(p_1p_2/p)=1$

กรณีที่ 2.2.1 $p\equiv -p_1p_2+4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 3 \pmod 8$ เนื่องจาก $4\nmid -p_1p_2+4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right)-3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.2.2 $p\equiv p_1p_2+4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 3 \pmod 8$ จะได้ว่า $p\equiv 4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p\equiv 3 \pmod 8$

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=3$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1\equiv 1 \pmod 8$ $\quad 8y_2\equiv 1 \pmod{p_1p_2}$ $\quad y_1=-1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$\begin{aligned} a_1m_1'y_1+a_2m_2'y_2 &= (3)(p_1p_2)(-1)+\left(4\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5) \\ &= -3p_1p_2+32n_5\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \end{aligned}$$

ดังนั้น $p\equiv -3p_1p_2+32n_5\left(n_3r_1^{S_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5\equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.3 $p\equiv -p_1p_2+4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 3 \pmod 8$ เนื่องจาก $4\nmid -p_1p_2+4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{T_2}p_1\right)-3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.2.4 $p\equiv p_1p_2+4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 3 \pmod 8$ จะได้ว่า $p\equiv 4\left(n_3r_1^{T_1}p_2+4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

และ $p \equiv 3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (3)(p_1p_2)(-1) + \left(4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= -3p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv -3p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.5 $p \equiv -p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-3)(p_1p_2)(-1) + \left(4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= 3p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv 3p_1p_2 + 32n_5\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

กรณีที่ 2.2.6 $p \equiv p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 4\left(n_3r_1^{S_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.2.7 $p \equiv -p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-3)(p_1p_2)(-1) + \left(4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= 3p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv 3p_1p_2 + 32n_5\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.8 $p \equiv p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 4\left(n_3r_1^{T_1}p_2 + 4(n+1)n_4r_2^{S_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

มหาวิทยาลัยรังสิต Rangsit University

จากกรณีทั้งหมดเราสรุปได้ว่า

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

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

$T_2\in\{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, 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

มหาวิทยาลัยราชภัฏสกลนคร

3.3 รูปแบบจำนวนเฉพาะคี่ p เมื่อ $p_1 \equiv 3 \pmod 4$ และ $p_2 \equiv 3 \pmod 4$

ทฤษฎีบท 3.3.1 : ให้ p_1 และ p_2 เป็นจำนวนเฉพาะคี่ โดยที่ $p_1 \equiv 3 \pmod 4$ และ $p_2 \equiv 3 \pmod 4$ เพราะฉะนั้นเราสามารถเขียน $p_1 = 4m+3$ และ $p_2 = 4n+3$ สำหรับบางจำนวนเต็ม m และ n

1. ถ้า $m+n$ เป็นจำนวนเต็มคู่ แล้ว $p_1 p_2 \equiv 1 \pmod 8$
2. ถ้า $m+n$ เป็นจำนวนเต็มคี่ แล้ว $-3p_1 p_2 \equiv 1 \pmod 8$

พิสูจน์ : 1 สมมติ $m+n$ เป็นจำนวนเต็มคู่ เราสามารถเขียน $m+n=2l$ สำหรับบางจำนวนเต็ม l

จะได้ว่า $p_1 p_2 = (4m+3)(4n+3) = 16mn+12(m+n)+9 = 16mn+12(2l)+8+1 = 8(2mn+3l+1)+1$

ดังนั้น $p_1 p_2 \equiv 1 \pmod 8$

2. สมมติ $m+n$ เป็นจำนวนเต็มคี่ เราสามารถเขียน $m+n=2l+1$ สำหรับบางจำนวนเต็ม l

จะได้ว่า $p_1 p_2 = (4m+3)(4n+3) = 16mn+12(m+n)+9 = 16mn+12(2l+1)+9 = 8(2mn+3l)+21$

เพราะฉะนั้น $-3p_1 p_2 = 8(-6mn-9l)-63 = 8(-6mn-9l)-64+1 = 8(-6mn-9l-8)+1$

ดังนั้น $-3p_1 p_2 \equiv 1 \pmod 8$

ทฤษฎีบท 3.3.2 : ให้ 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 $p \nmid p_2$ เพราะฉะนั้นเราสามารถเขียน $p_1 = 4m+3$ และ $p_2 = 4n+3$ สำหรับบางจำนวนเต็ม m และ n

มหาวิทยาลัยราชภัฏเพชรบุรี

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

$T_2\in\{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, 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

มหาวิทยาลัยรามคำแหง

2. ถ้า $m+n$ เป็นจำนวนเต็มคี่ แล้ว

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

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

$T_2\in\{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, 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

มหาวิทยาลัยรามคำแหง

พิสูจน์ จากทฤษฎีบท เราทราบว่า

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

เมื่อ $S_1\in\{2,\ 4,\ 6,\ \ldots,\ p_1-1\}$, $S_2\in\{2,\ 4,\ 6,\ \ldots,\ p_2-1\}$, $T_1\in\{1,\ 3,\ 5,\ \ldots,\ p_1-2\}$, $T_2\in\{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, r_1 และ r_2 เป็นรากปฐมฐานมอดุโล p_1 และ p_2 ตามลำดับ และ n_0, m_0, n_3 และ n_4 เป็นจำนวนเต็มที่สอดคล้อง $p_1=4n_0-1$, $p_2=4m_0-1$, $4p_2n_3\equiv 1\pmod{p_1}$ และ $4p_1n_4\equiv 1\pmod{p_2}$ ตามลำดับ

และ $(2/p)=\begin{cases}1, & p\equiv\pm1\pmod 8\\ -1, & p\equiv\pm3\pmod 8\end{cases}$ เพราะฉะนั้น $m_0=m+1$ และ $n_0=n+1$ ส่งผลให้

$$(p_1p_2/p)\equiv\begin{cases}1, & p\equiv p_1p_2+16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)\pmod{4p_1p_2}\\ & \equiv -p_1p_2+16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)\pmod{4p_1p_2}\\ & \equiv p_1p_2+16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)\pmod{4p_1p_2}\\ & \equiv -p_1p_2+16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)\pmod{4p_1p_2}\\ -1, & p\equiv p_1p_2+16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)\pmod{4p_1p_2}\\ & \equiv -p_1p_2+16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)\pmod{4p_1p_2}\\ & \equiv p_1p_2+16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)\pmod{4p_1p_2}\\ & \equiv -p_1p_2+16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)\pmod{4p_1p_2}\end{cases}$$

เมื่อ $S_1\in\{2,\ 4,\ 6,\ \ldots,\ p_1-1\}$, $S_2\in\{2,\ 4,\ 6,\ \ldots,\ p_2-1\}$, $T_1\in\{1,\ 3,\ 5,\ \ldots,\ p_1-2\}$, $T_2\in\{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, r_1 และ r_2 เป็นรากปฐมฐานมอดุโล p_1 และ p_2 ตามลำดับ และ n_3 และ n_4 เป็นจำนวนเต็มที่สอดคล้อง $4p_2n_3\equiv 1\pmod{p_1}$ และ $4p_1n_4\equiv 1\pmod{p_2}$ ตามลำดับ

มหาวิทยาลัยราชภัฏเพชรบุรี

1. สมมติ $m+n$ เป็นจำนวนเต็มคู่ จะได้ว่า

กรณีที่ 1 พิจารณา $(2p_1p_2/p)=1$

จากทฤษฎีบท จะได้ว่า $(2/p)(p_1p_2/p)=1$

กรณีที่ 1.1 $(2/p)=1$ และ $(p_1p_2/p)=1$

กรณีที่ 1.1.1 $p\equiv p_1p_2+16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)\pmod{4p_1p_2}$ และ

$p\equiv 1 \pmod 8$ จะได้ว่า $p\equiv 16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)\pmod{p_1p_2}$

และ $p\equiv 1 \pmod 8$

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=1$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1\equiv 1\pmod 8$ $\quad 8y_2\equiv 1\pmod{p_1p_2}$ $\quad y_1=1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1+a_2m_2'y_2=(1)(p_1p_2)(1)+\left(16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$=p_1p_2+128n_5\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p\equiv p_1p_2+128n_5\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)\pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5\equiv 1\pmod{p_1p_2}$

กรณีที่ 1.1.2 $p\equiv -p_1p_2+16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)\pmod{4p_1p_2}$ และ

$p\equiv 1 \pmod 8$ เนื่องจาก $4\nmid -p_1p_2+16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)-1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.3 $p\equiv p_1p_2+16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)\pmod{4p_1p_2}$ และ

$p\equiv 1 \pmod 8$ จะได้ว่า $p\equiv 16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)\pmod{p_1p_2}$

และ $p\equiv 1 \pmod 8$

มหาวิทยาลัยรามคำแหง

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (1)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.1.4 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 1 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - 1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.5 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.6 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

มหาวิทยาลัยราชภัฏพิบูลสงคราม

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-1)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= -p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv -p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.1.7 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.8 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-1)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= -p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv -p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

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

กรณีที่ 1.2.1 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 3 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - 3$

มหาวิทยาลัยราชภัฏเทพสตรี

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.2.2 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 3 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8 \qquad m_1' = p_1p_2 \qquad a_1 = 3$

$m_2 = p_1p_2 \qquad m_2' = 8 \qquad a_2 = 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8 \qquad 8y_2 \equiv 1 \pmod{p_1p_2} \qquad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (3)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.3 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 3 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) - 3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.2.4 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 3 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8 \qquad m_1' = p_1p_2 \qquad a_1 = 3$

$m_2 = p_1p_2 \qquad m_2' = 8 \qquad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8 \qquad 8y_2 \equiv 1 \pmod{p_1p_2} \qquad y_1 = 1$

มหาวิทยาลัยราชภัฏสวนสุนันทา

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (3)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.5 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-3)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= -3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv -3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.6 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.2.7 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -3 \pmod 8$

มหาวิทยาลัยราชภัฏเทพสตรี

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-3)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= -3p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv -3p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.8 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

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

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

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

กรณีที่ 2.1.1 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 1 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (1)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$$

มหาวิทยาลัยราชภัฏพิบูลสงคราม

ดังนั้น $p \equiv p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.2 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 1 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) - 1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.1.3 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 1 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (1)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.4 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 1 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - 1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

มหาวิทยาลัยราชภัฏเพชรบุรี

กรณีที่ 2.1.5 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.1.6 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-1)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$

$$= -p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv -p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.7 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.1.8 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

มหาวิทยาลัยราชภัฏเพชรบุรี

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-1)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= -p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv -p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2 $(2/p) = -1$ และ $(p_1p_2/p) = 1$

กรณีที่ 2.2.1 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 3 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - 3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.2.2 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 3 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (3)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

กรณีที่ 2.2.3 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 3 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) - 3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.2.4 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 3 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (3)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.5 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-3)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= -3p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$$

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

ดังนั้น $p \equiv -3p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.6 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.2.7 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = 1$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-3)(p_1p_2)(1) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= -3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv -3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.8 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

มหาวิทยาลัยราชภัฏเพชรบุรี

จากกรณีทั้งหมดเราสรุปได้ว่า

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

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

$T_2\in\{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, 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

มหาวิทยาลัยเกษตรศาสตร์

2. สมมติ $m+n$ เป็นจำนวนเต็มคี่ จะได้ว่า

กรณีที่ 1 พิจารณา $(2p_1p_2/p)=1$

จากทฤษฎีบท จะได้ว่า $(2/p)(p_1p_2/p)=1$

กรณีที่ 1.1 $(2/p)=1$ และ $(p_1p_2/p)=1$

กรณีที่ 1.1.1 $p\equiv p_1p_2+16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 1 \pmod 8$ จะได้ว่า $p\equiv 16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p\equiv 1 \pmod 8$

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=1$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1\equiv 1 \pmod 8$ $\quad 8y_2\equiv 1 \pmod{p_1p_2}$ $\quad y_1=-3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1+a_2m_2'y_2=(1)(p_1p_2)(-3)+\left(16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$=-3p_1p_2+128n_5\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p\equiv -3p_1p_2+128n_5\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$ เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5\equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.1.2 $p\equiv -p_1p_2+16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 1 \pmod 8$ เนื่องจาก $4\nmid -p_1p_2+16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)-1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.3 $p\equiv p_1p_2+16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p\equiv 1 \pmod 8$ จะได้ว่า $p\equiv 16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p\equiv 1 \pmod 8$

มหาวิทยาลัยราชภัฏเทพสตรี

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (1)(p_1p_2)(-3) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= -3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv -3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.1.4 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 1 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - 1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.5 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.6 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

มหาวิทยาลัยราชภัฏพิบูลสงคราม

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-1)(p_1p_2)(-3) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.1.7 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.1.8 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-1)(p_1p_2)(-3) + \left(16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

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

กรณีที่ 1.2.1 $p\equiv p_1p_2+16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)\pmod{4p_1p_2}$ และ

$p\equiv 3 \pmod 8$ เนื่องจาก $4\nmid p_1p_2+16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)-3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.2.2 $p\equiv -p_1p_2+16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)\pmod{4p_1p_2}$ และ

$p\equiv 3 \pmod 8$ จะได้ว่า $p\equiv 16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)\pmod{p_1p_2}$

และ $p\equiv 3 \pmod 8$

$m_1=8$ $\quad m_1'=p_1p_2$ $\quad a_1=3$

$m_2=p_1p_2$ $\quad m_2'=8$ $\quad a_2=16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1\equiv 1\pmod 8$ $\quad 8y_2\equiv 1\pmod{p_1p_2}$ $\quad y_1=-3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1+a_2m_2'y_2=(3)(p_1p_2)(-3)+\left(16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$=-9p_1p_2+128n_5\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p\equiv -p_1p_2+128n_5\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)\pmod{8p_1p_2}$ 3

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5\equiv 1\pmod{p_1p_2}$

กรณีที่ 1.2.3 $p\equiv p_1p_2+16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)\pmod{4p_1p_2}$ และ

$p\equiv 3 \pmod 8$ เนื่องจาก $4\nmid p_1p_2+16\left((n+1)n_3r_1^{S_1}p_2+(m+1)n_4r_2^{T_2}p_1\right)-3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 1.2.4 $p\equiv -p_1p_2+16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)\pmod{4p_1p_2}$ และ

$p\equiv 3 \pmod 8$ จะได้ว่า $p\equiv 16\left((n+1)n_3r_1^{T_1}p_2+(m+1)n_4r_2^{S_2}p_1\right)\pmod{p_1p_2}$

และ $p\equiv 3 \pmod 8$

มหาวิทยาลัยราชภัฏพิบูลสงคราม

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (3)(p_1p_2)(-3) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= -9p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv -p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.5 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-3)(p_1p_2)(-3) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= 9p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.6 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

มหาวิทยาลัยรามคำแหง

กรณีที่ 1.2.7 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-3)(p_1p_2)(-3) + \left(16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= 9p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 1.2.8 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

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

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

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

กรณีที่ 2.1.1 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 1 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

มหาวิทยาลัยราชภัฏเพชรบุรี

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (1)(p_1p_2)(-3) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= -3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv -3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.2 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 1 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) - 1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.1.3 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 1 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 1 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (1)(p_1p_2)(-3) + \left(16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= -3p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv -3p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.4 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv 1 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - 1$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

มหาวิทยาลัยราชภัฏเทพสตรี

กรณีที่ 2.1.5 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.1.6 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

$m_1 = 8 \qquad m_1' = p_1p_2 \qquad a_1 = -1$

$m_2 = p_1p_2 \qquad m_2' = 8 \qquad a_2 = 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8 \qquad 8y_2 \equiv 1 \pmod{p_1p_2} \qquad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-1)(p_1p_2)(-3) + \left(16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.1.7 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) - (-1)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.1.8 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -1 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -1 \pmod 8$

มหาวิทยาลัยราชภัฏเทพสตรี

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -1$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-1)(p_1p_2)(-3) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv 3p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2 $(2/p) = -1$ และ $(p_1p_2/p) = 1$

กรณีที่ 2.2.1 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 3 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - 3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.2.2 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 3 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = 3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (3)(p_1p_2)(-3) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= -9p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv -p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

มหาวิทยาลัยราชภัฏเทพสตรี

กรณีที่ 2.2.3 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 3 \pmod 8$ เนื่องจาก $4 \nmid p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) - 3$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.2.4 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv 3 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv 3 \pmod 8$

$m_1 = 8 \qquad m_1' = p_1p_2 \qquad a_1 = 3$

$m_2 = p_1p_2 \qquad m_2' = 8 \qquad a_2 = 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8 \qquad 8y_2 \equiv 1 \pmod{p_1p_2} \qquad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (3)(p_1p_2)(-3) + \left(16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= -9p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$$

ดังนั้น $p \equiv -p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.5 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ

$p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -3 \pmod 8$

$m_1 = 8 \qquad m_1' = p_1p_2 \qquad a_1 = -3$

$m_2 = p_1p_2 \qquad m_2' = 8 \qquad a_2 = 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8 \qquad 8y_2 \equiv 1 \pmod{p_1p_2} \qquad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-3)(p_1p_2)(-3) + \left(16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)\right)(8)(n_5)$$
$$= 9p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right)$$

มหาวิทยาลัยการกีฬาแห่งชาติ

ดังนั้น $p \equiv p_1p_2 + 128n_5\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.6 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

กรณีที่ 2.2.7 $p \equiv p_1p_2 + 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -3 \pmod 8$ จะได้ว่า $p \equiv 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{p_1p_2}$

และ $p \equiv -3 \pmod 8$

$m_1 = 8$ $\quad m_1' = p_1p_2$ $\quad a_1 = -3$

$m_2 = p_1p_2$ $\quad m_2' = 8$ $\quad a_2 = 16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$

$p_1p_2y_1 \equiv 1 \pmod 8$ $\quad 8y_2 \equiv 1 \pmod{p_1p_2}$ $\quad y_1 = -3$

โดยทฤษฎีบทเศษเหลือของจีน จะได้ว่า

$$a_1m_1'y_1 + a_2m_2'y_2 = (-3)(p_1p_2)(-3) + \left(16\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)\right)(8)(n_5)$$
$$= 9p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right)$$

ดังนั้น $p \equiv p_1p_2 + 128n_5\left((n+1)n_3r_1^{T_1}p_2 + (m+1)n_4r_2^{T_2}p_1\right) \pmod{8p_1p_2}$

เมื่อ n_5 เป็นจำนวนเต็มที่ทำให้ $8n_5 \equiv 1 \pmod{p_1p_2}$

กรณีที่ 2.2.8 $p \equiv -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) \pmod{4p_1p_2}$ และ $p \equiv -3 \pmod 8$ เนื่องจาก $4 \nmid -p_1p_2 + 16\left((n+1)n_3r_1^{S_1}p_2 + (m+1)n_4r_2^{S_2}p_1\right) - (-3)$

ดังนั้น ระบบสมภาคนี้ไม่มีผลเฉลย

มหาวิทยาลัยรามคำแหง

จากกรณีทั้งหมดเราสรุปได้ว่า

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

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

$T_2\in\{1,\ 3,\ 5,\ \ldots,\ p_2-2\}$, 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

บทที่ 4
สรุปผลการวิจัยและข้อเสนอแนะ

4.1 สรุปผลการวิจัย

เนื้อหาในงานวิจัยนี้กล่าวถึงรูปแบบจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ $(2p_1p_2 / p)$ เมื่อ p_1, p_2 เป็นจำนวนเฉพาะคี่, $p \nmid p_1$ และ $p \nmid p_2$ โดยในการหารูปแบบจำนวนเฉพาะนี้เราใช้ทฤษฎีบทเศษเหลือของจีนช่วยในการแก้ระบบสมภาคในแต่ละกรณีย่อยจนครบทุกกรณี โดยเริ่มต้นที่แบ่งการพิจารณาจำนวนเฉพาะ p_1 และ p_2 ออกเป็น 3 กรณีดังต่อไปนี้

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

ในกรณีนี้ เราได้รูปแบบจำนวนเฉพาะคี่ p สองรูปแบบโดยแบ่งการพิจารณาเป็น

$m+n$ เป็นจำนวนเต็มคู่ และ $m+n$ เป็นจำนวนเต็มคี่ เมื่อ $p_1 = 4m+1$ และ $p_2 = 4n+1$ สำหรับบางจำนวนเต็ม m และ n

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

ในกรณีนี้ เราได้รูปแบบจำนวนเฉพาะคี่ p สองรูปแบบโดยแบ่งการพิจารณาเป็น

$3m+n$ เป็นจำนวนเต็มคู่ และ $3m+n$ เป็นจำนวนเต็มคี่ $p_1 = 4m+1$ และ $p_2 = 4n+3$ สำหรับบางจำนวนเต็ม m และ n

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

ในกรณีนี้ เราได้รูปแบบจำนวนเฉพาะคี่ p สองรูปแบบโดยแบ่งการพิจารณาเป็น

$m+n$ เป็นจำนวนเต็มคู่ และ $m+n$ เป็นจำนวนเต็มคี่ เมื่อ $p_1 = 4m+1$ และ $p_2 = 4n+1$ สำหรับบางจำนวนเต็ม m และ n

ดังนั้นจากทั้งสามกรณี เราพบรูปแบบจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ $(2p_1p_2 / p)$ เมื่อ p_1, p_2 เป็นจำนวนเฉพาะคี่, $p \nmid p_1$ และ $p \nmid p_2$ ครบทุกรูปแบบของ p_1 และ p_2

มหาวิทยาลัยราชภัฏเทพสตรี

4.2 ข้อเสนอแนะ

จากการศึกษาเอกสารงานวิจัยก่อนหน้านี้ รวมถึงการวิจัยครั้งนี้ เราได้รูปแบบจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ต่อไปนี้

1. $(2/p)$
2. (p_1/p) เมื่อ p_1 เป็นจำนวนเฉพาะคี่ โดยที่ $p \nmid p_1$
3. $(2p_1/p)$ เมื่อ p_1 เป็นจำนวนเฉพาะคี่ โดยที่ $p \nmid p_1$
4. (p_1p_2/p) เมื่อ p_1 และ p_2 เป็นจำนวนเฉพาะคี่ โดยที่ $p \nmid p_1$ และ $p \nmid p_2$
5. $(2p_1p_2/p)$ เมื่อ p_1 และ p_2 เป็นจำนวนเฉพาะคี่ โดยที่ $p \nmid p_1$ และ $p \nmid p_2$

ดังนั้นงานวิจัยชิ้นนี้ยังสามารถพัฒนาต่อไปในรูปแบบอื่นๆเช่น

$(p_1p_2p_3/p)$ เมื่อ p_1, p_2 และ p_3 เป็นจำนวนเฉพาะคี่ โดยที่ $p \nmid p_1, p \nmid p_2$ และ $p \nmid p_3$

$(2p_1p_2p_3/p)$ เมื่อ p_1, p_2 และ p_3 เป็นจำนวนเฉพาะคี่ โดยที่ $p \nmid p_1, p \nmid p_2$ และ $p \nmid p_3$

หรือขยายจนถึงรูปทั่วไปคือ

$\left(2p_1^{n_1}p_2^{n_2}p_3^{n_3}\cdots p_m^{n_m}/p\right)$ เมื่อ $p_1, p_2, \ldots, p_m$ เป็นจำนวนเฉพาะคี่ โดยที่ $p \nmid p_i$ ทุก $i \in \{1,2,3,\ldots,m\}$

มหาวิทยาลัยราชภัฏเทพสตรี

บรรณานุกรม

[1] อัจฉรา หาญชูวงศ์, "ทฤษฎีจำนวน", โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2542.

[2] อภิรัฐ ศิระวรกุล, "จำนวนเฉพาะ p ที่ทำให้ $\det(adj\ X) = b$ มีผลเฉลยใน $M_3(\mathbb{Z}_p)$", โครงงานระดับปริญญาตรี สาขาวิชาคณิตศาสตร์, จุฬาลงกรณ์มหาวิทยาลัย, 2547.

[3] อภิรัฐ ศิระวรกุล, จันทนา วรรณพันธุ์ และ นภาลัย สีสด "รูปแบบจำนวนเฉพาะคี่ p ในสัญลักษณ์เลอจองด์ (p_1p_2 / p)" การประชุมวิชาการระดับชาติมหาวิทยาลัยราชภัฏกลุ่มศรีอยุธยาครั้งที่ 7

มหาวิทยาลัยราชภัฏเทพสตรี