



วารสารคณิตศาสตร์ MJ-MATH 63(695) พฤษภาคม – สิงหาคม 2561

โดย สมาคมคณิตศาสตร์แห่งประเทศไทย ในพระบรมราชูปถัมภ์

<http://www.mathassociation.net>

Email: MathThaiOrg@gmail.com



ไดกราฟที่เกิดจากความสัมพันธ์ $a^4 \equiv b \pmod{n}$

Digraphs Arising from the Relation $a^4 \equiv b \pmod{n}$

รตินันท์ บุญเคลือบ และ ธัญพิชชา ยอดแก้ว

Ratinan Boonklurb¹ and Thunpisch Yodkaew²

¹Department of Mathematics and Computer Science, Faculty of Science,
Chulalongkorn University, Bangkok, 10330

²Department of Mathematics and Computer Science, Faculty of Science,
Chulalongkorn University, Bangkok, 10330

Email: ¹ratinan.b@chula.ac.th ²y.thunpisch@gmail.com

บทคัดย่อ

บทความฉบับนี้ศึกษาสมบัติและโครงสร้างของไดกราฟ $\Gamma(n, 4)$ ที่มีจุดยอดเป็นเซต $V = \{0, 1, 2, \dots, n-1\}$ และเส้นเชื่อมแสดงทิศทาง $(a, b) \in E \subseteq V \times V$ เมื่อ $a^4 \equiv b \pmod{n}$ โดย n เป็นจำนวนนับที่ $n \geq 2$ และหาสูตรของจำนวนจุดตรึงในไดกราฟดังกล่าว

คำสำคัญ: ไดกราฟ สมภาค จุดตรึง

ABSTRACT

This article studies properties and structure of the digraph $\Gamma(n, 4)$ which has the vertex set $V = \{0, 1, 2, \dots, n-1\}$ and directed edges $(a, b) \in E \subseteq V \times V$ if and only if $a^4 \equiv b \pmod{n}$ where n is an integer such that $n \geq 2$ and find the number of fixed point of this digraph.

Keywords: Digraph, Congruence, Fixed Point

บทความฉบับนี้ศึกษาเกี่ยวกับกราฟระบุทิศทางหรือไดกราฟที่ได้จากความสัมพันธ์สมภาค
ระหว่างจำนวนนับสองจำนวน

เช่น สำหรับไดกราฟ $G = (V, E)$ ถ้า $(a, b) \in E$ หมายความว่า มีเส้นเชื่อมจากจุดยอด a ไปยังจุดยอด b โดยเรียก a ว่าจุดเริ่มต้น และเรียก b ว่าจุดปลายของเส้นเชื่อมระบุทิศทาง และมักเขียนลูกศรกำกับทิศทางไว้ ในขณะที่ถ้า $(a, a) \in E$ จะหมายถึง มีเส้นเชื่อมม้วนเป็นวงกลับมาที่จุดยอด a โดยเรียกเส้นเชื่อมลักษณะนี้ว่าวงวนและเรียก a ว่าเป็นจุดตรึงของไดกราฟ G

สังเกตว่าใน G มี $(0,0), (1,1) \in E$ เป็นจุดตรึงของ G ซึ่งในแผนภาพแทนด้วยเส้นเชื่อมแสดงทิศทางที่มีลักษณะเป็นวงวนดังรูป 1.1 และมี $(2,16), (16,9), (9,6), (6,8), (8,2) \in E$ ซึ่งในแผนภาพแทนด้วยเส้นเชื่อมแสดงทิศทางห้าเส้นที่เชื่อมจุดยอด 2, 16, 9, 6 และ 8 เข้าด้วยกันเป็นวง เรียกเส้นเชื่อมแสดงทิศทางทั้งห้าเส้นที่เชื่อมจุดยอดเหล่านี้เข้าด้วยกันว่า วง

10

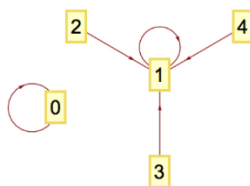
เชื่อมระบุทิศทาง (a, b) ในไดกราฟเป็น $a^5 \equiv b \pmod{n}$ และในปี ค.ศ. 2011 Somer และ Křizek [4] ได้ขยายแนวคิดของ [2] มาศึกษาไดกราฟ $\Gamma(n, k)$ ที่เงื่อนไขการมีเส้นเชื่อมระบุทิศทาง (a, b) ในไดกราฟเป็น $a^k \equiv b \pmod{n}$ เมื่อ k เป็นจำนวนนับที่ $k \geq 2$ ใดๆก็ได้ [4] พิสูจน์ได้เพียงขอบเขตล่างของจำนวนจุดตรึงของไดกราฟ $\Gamma(n, k)$ เท่านั้น

2. จุดตรึงและสูตรสำหรับจำนวนจุดตรึงของไดกราฟ $\Gamma(n, 4)$ ที่เกิดจากความสัมพันธ์

$$a^4 \equiv b \pmod{n}$$

ให้ n เป็นจำนวนนับที่ $n \geq 2$ และ $V = \{0, 1, 2, \dots, n-1\}$ นิยามไดกราฟ $\Gamma(n, 4) = (V, E)$ โดย $(a, b) \in E$ เมื่อ $a^4 \equiv b \pmod{n}$

ตัวอย่าง 2.1 ให้ $n = 5$ จะได้ว่า $V = \{0, 1, 2, 3, 4\}$ เนื่องจาก $0^4 \equiv 0 \pmod{5}$, $1^4 \equiv 1 \pmod{5}$, $2^4 \equiv 1 \pmod{5}$, $3^4 \equiv 1 \pmod{5}$ และ $4^4 \equiv 1 \pmod{5}$ ดังนั้น $\Gamma(5, 4)$ จะมีแผนภาพดังรูป 2.1



รูปที่ 2.1 $\Gamma(5, 4)$

บทนิยาม 2.1 จุดยอด v ของไดกราฟ $\Gamma(n, 4)$ เป็นจุดตรึงเอกเทศ เมื่อ v เป็นจุดตรึงของ $\Gamma(n, 4)$ ที่ไม่มีเส้นเชื่อมระบุทิศทางจากจุดยอดอื่นของ $\Gamma(n, 4)$ มาเชื่อมกับ v

ทฤษฎีบท 2.1 0 และ 1 เป็นจุดตรึงของ $\Gamma(n, 4)$ ยิ่งไปกว่านั้น 0 เป็นจุดตรึงเอกเทศของ $\Gamma(n, 4)$ ก็ต่อเมื่อ n ปราสจากกำลังสอง นั่นคือ n มีสมบัติว่าสำหรับจำนวนเฉพาะ p ที่เป็นตัวประกอบของ n ถ้า $p^\alpha | n$ แล้ว $\alpha = 1$

บทพิสูจน์ เนื่องจาก $n | (0^4 - 0)$ และ $n | (1^4 - 1)$ ทุกจำนวนนับ n จะได้ว่า 0 และ 1 เป็นจุดตรึงของ $\Gamma(n, 4)$

ต่อมาจะพิสูจน์ว่า 0 เป็นจุดตรึงเอกเทศของ $\Gamma(n, 4)$ ก็ต่อเมื่อ n ปราสจากกำลังสอง

สมมติว่า n ไม่ปราสจากกำลังสอง จะได้ว่ามีจำนวนเฉพาะ p และจำนวนเต็ม k ที่ $n = p^2 k$ ทำให้ $\left(\frac{n}{p}\right)^4 = n^2 k^2 \equiv 0 \pmod{n}$ ดังนั้น $\left(\frac{n}{p}, 0\right) \in E$ นั่นคือ 0 ไม่เป็นจุดตรึงเอกเทศของ $\Gamma(n, 4)$

สมมติว่า n ปราสจากกำลังสอง ทำให้ได้ว่ามีจำนวนเฉพาะ $p_1, p_2, p_3, \dots, p_l$ ที่ $n = p_1 p_2 p_3 \dots p_l$ ต่อมาสมมติว่า 0 ไม่เป็นจุดตรึงเอกเทศ ฉะนั้นจะมี $k \in V$ และมีจำนวนเต็ม s ที่ $k^4 = p_1 p_2 p_3 \dots p_l s$ เนื่องจาก k เป็นจำนวนเต็ม ดังนั้นจะมีจำนวนเต็ม t ที่ทำให้

$$k^4 = p_1 p_2 p_3 \dots p_l (p_1 p_2 p_3 \dots p_l)^3 t^4$$

จะได้ว่า $k = p_1 p_2 p_3 \dots p_l t \geq n$ ทำให้เกิดข้อขัดแย้ง □

ข้อสังเกต 2.1 เนื่องจาก $(n-1)^4 - (n-1) = (n-1)(n^3 - 3n^2 + 3n - 2)$ ทำให้ได้ว่า n หาร $(n-1)^4 - (n-1)$ ลงตัว ก็ต่อเมื่อ $n = 2$ ดังนั้นสำหรับจำนวนนับ n ที่ $n \geq 3$ จุดยอด $n-1$ ไม่เป็นจุดตรึงของ $\Gamma(n, 4)$ ซึ่งแตกต่างจากไคกราฟที่ศึกษาใน [2] และ [3] ที่ $n-1$ เป็นจุดตรึงของไคกราฟเสมอ

ต่อมาในการหาสูตรสำหรับจำนวนจุดตรึงทั้งหมดใน $\Gamma(n, 4)$ จำเป็นต้องมีความรู้พื้นฐานทางทฤษฎีจำนวนเกี่ยวกับการมีอยู่ของผลเฉลยของสมภาค $f(x) \equiv 0 \pmod{m}$

ทฤษฎีบทประกอบ 2.2 [5] (ทฤษฎีบทประกอบของเฮนเซล) ให้ $f(x)$ เป็นพหุนามในตัวแปร x ที่มีสัมประสิทธิ์เป็นจำนวนเต็มและ r เป็นจำนวนนับ

ถ้าจำนวนเต็ม $m_1, m_2, m_3, \dots, m_r$ เป็นจำนวนเฉพาะสัมพัทธ์ซึ่งกันและกัน และ $m = m_1 m_2 m_3 \dots m_r$ แล้ว $f(x) \equiv 0 \pmod{m}$ มีผลเฉลย ก็ต่อเมื่อ $f(x) \equiv 0 \pmod{m_i}$ มีผลเฉลยทุก $i \in \{1, 2, 3, \dots, r\}$ ยิ่งไปกว่านั้นถ้า $v(m)$ และ $v(m_i)$ เป็นจำนวนผลเฉลยของ $f(x) \equiv 0 \pmod{m}$ และ $f(x) \equiv 0 \pmod{m_i}$ ตามลำดับ แล้ว

$$v(m) = v(m_1)v(m_2)v(m_3) \dots v(m_r)$$

นอกจากนี้ยังต้องอาศัยความรู้เกี่ยวกับส่วนตกค้างกำลังสองมอดุโล m

บทนิยาม 2.2 [6]

(ก) ให้ m เป็นจำนวนเต็มบวกและ a เป็นจำนวนเต็มที่ทั้งคู่เป็นจำนวนเฉพาะสัมพัทธ์ซึ่งกันและกัน จะกล่าวว่า a เป็นส่วนตกค้างกำลังสองมอดุโล m เมื่อ $x^2 \equiv a \pmod{m}$ มีผลเฉลย มิเช่นนั้นจะกล่าวว่า a ไม่เป็นส่วนตกค้างกำลังสองมอดุโล m

(ข) ให้ p เป็นจำนวนเฉพาะคี่และ a เป็นจำนวนเต็มที่ $p \nmid a$ สัญลักษณ์เลอช็องดร์ (a/p) กำหนดค่าโดย

$$(a/p) = \begin{cases} 1 & \text{เมื่อ } a \text{ เป็นส่วนตกค้างกำลังสองมอดุโล } p \\ -1 & \text{เมื่อ } a \text{ ไม่เป็นส่วนตกค้างกำลังสองมอดุโล } p \end{cases}$$

ทั้งนี้สัญลักษณ์เลอช็องดร์มีสมบัติสำคัญดังต่อไปนี้

ทฤษฎีบทประกอบ 2.3 [6] ให้ p เป็นจำนวนเฉพาะคี่และ a และ b เป็นจำนวนเต็มที่ $p \nmid a$ และ $p \nmid b$

$$(ก) (ab/p) = (a/p)(b/p)$$

$$(ข) (-1/p) = \begin{cases} 1 & \text{เมื่อ } p \equiv 1 \pmod{4} \\ -1 & \text{เมื่อ } p \equiv 3 \pmod{4} \end{cases} \text{ และ}$$

$$\text{ถ้า } p \neq 3 \text{ แล้ว } (3/p) = \begin{cases} 1 & \text{เมื่อ } p \equiv 1 \text{ หรือ } -1 \pmod{12} \\ -1 & \text{เมื่อ } p \equiv 5 \text{ หรือ } -5 \pmod{12} \end{cases}$$

ทฤษฎีบทประกอบ 2.3 ทำให้เราสามารถคำนวณค่า $(-3/p)$ เมื่อ p เป็นจำนวนเฉพาะคี่ที่ $p \neq 3$ ได้

ทฤษฎีบทประกอบ 2.4 ให้ p เป็นจำนวนเฉพาะคี่ที่ $p \neq 3$ จะได้ว่า

$$(-3/p) = \begin{cases} 1 & \text{เมื่อ } p \equiv 1 \text{ หรือ } 7 \pmod{12} \\ -1 & \text{เมื่อ } p \equiv 5 \text{ หรือ } 11 \pmod{12} \end{cases}$$

บทพิสูจน์ ให้ p เป็นจำนวนเฉพาะคี่ที่ $p \neq 3$ จะได้ว่า $(-3/p) = (3/p)(-1/p)$

กรณี 1 $p \equiv 1 \pmod{12}$ จะได้ว่า $p \equiv 1 \pmod{4}$

$$\text{ดังนั้น } (-3/p) = 1 \cdot 1 = 1$$

กรณี 2 $p \equiv 7 \pmod{12}$ จะได้ว่า $p \equiv 3 \pmod{4}$

$$\text{ดังนั้น } (-3/p) = (-1) \cdot (-1) = 1$$

กรณี 3 $p \equiv 5 \pmod{12}$ จะได้ว่า $p \equiv 1 \pmod{4}$

$$\text{ดังนั้น } (-3/p) = (-1) \cdot 1 = -1$$

กรณี 4 $p \equiv 11 \pmod{12}$ จะได้ว่า $p \equiv 3 \pmod{4}$

$$\text{ดังนั้น } (-3/p) = 1 \cdot (-1) = -1$$

□

ทฤษฎีบทต่อไปนี้เป็นสูตรสำหรับหาจำนวนจุดตรึงทั้งหมดใน $\Gamma(n, 4)$

ทฤษฎีบท 2.5 ให้ n เป็นจำนวนนับที่ $n \geq 2$ ที่แยกตัวประกอบได้ในรูป

$$n = 2^m p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_s^{\alpha_s}$$

โดยที่ $p_1 < p_2 < p_3 < \dots < p_s$ เป็นจำนวนเฉพาะที่ต่างกัน $\alpha_i \geq 1, m \geq 0$ และ $s \geq 0$ และให้ $\omega(n)$ แทนจำนวนของจำนวนเฉพาะที่ p_i ที่เป็นตัวประกอบของ n และ $p_i \equiv 1$ หรือ $7 \pmod{12}$ ถ้า $L(n)$ แทนจำนวนจุดตรึงทั้งหมดใน $\Gamma(n, 4)$ แล้ว

$$L(n) = \begin{cases} 2^{\omega(n)+s} & \text{เมื่อ } m = 0 \\ 2^{\omega(n)+s+1} & \text{เมื่อ } m \geq 1 \end{cases}$$

บทพิสูจน์ เนื่องจาก $L(n)$ เป็นจำนวนจุดตรึงทั้งหมดใน $\Gamma(n, 4)$ ดังนั้น

$$L(n) = |\{0 \leq k < n-1 : f(k) \equiv 0 \pmod{n}\}|$$

เป็นจำนวนผลเฉลยใน V ของ $f(x) = x^4 - x = x(x-1)(x^2 + x + 1) \equiv 0 \pmod{n}$

กรณี 1 $m = 0$

กรณี 1.1 $s = 1$ นั่นคือ $n = p_1^{\alpha_1}$

โดยไม่เสียไร้วัยไปให้ $n = p^\alpha$ เมื่อ p เป็นจำนวนเฉพาะที่ และ α เป็นจำนวนนับ

จะได้ว่า $V = \{0, 1, 2, \dots, p^\alpha - 1\}$

สมมติให้ $x \in V - \{0, 1\}$ เป็นผลเฉลยของ $f(x) \equiv 0 \pmod{p^\alpha}$

เนื่องจาก $p|p^\alpha$ ทำให้ได้ว่า $p|x$ หรือ $p|(x-1)$ หรือ $p|(x^2 + x + 1)$

กรณี 1.1.1 $p|x$

สมมติว่า $p|(x-1)$ หรือ $p|(x^2 + x + 1)$ จะได้ว่า $p|1$ ทำให้เกิดข้อขัดแย้ง

ดังนั้น $p \nmid (x-1)$ และ $p \nmid (x^2 + x + 1)$ ทำให้ได้ด้วยว่า $p^\alpha \nmid (x-1)$ และ $p^\alpha \nmid (x^2 + x + 1)$

และเนื่องจาก $2 \leq x \leq p^\alpha - 1$ ทำให้ได้ว่า $p^\alpha \nmid x$ เช่นกัน

กรณี 1.1.2 $p|(x-1)$

ในทำนองเดียวกันกับกรณี 1.1.1 สามารถพิสูจน์ได้ว่า $p^\alpha \nmid x, p^\alpha \nmid (x-1)$ และ

$p^\alpha \nmid (x^2 + x + 1)$

กรณี 1.1.3 $p|(x^2 + x + 1)$

เนื่องจาก $4(x^2 + x + 1) = (2x + 1)^2 + 3$ ทำให้ $p|(x^2 + x + 1)$ ส่งผลให้เกิดความสัมพันธ์

$y^2 \equiv -3 \pmod{p}$ ถ้า $p = 3$ แล้วเห็นได้ชัดว่า $y^2 \equiv -3 \pmod{p}$ ไม่มีผลเฉลย แต่เมื่อ $p \neq 3$

และ $p \equiv 1$ หรือ $7 \pmod{12}$ โดยทฤษฎีบทประกอบ 2.4 จะได้ว่า $y^2 \equiv -3 \pmod{p}$ มีผลเฉลย

สองตัว สมมติว่าเป็น a และ b ที่แตกต่างกัน

ดังนั้นจากกรณี 1.1.1, 1.1.2 และ 1.1.3 จะได้ว่า

$$L(n) = \begin{cases} |\{0,1,a,b\}| = 4 & \text{เมื่อ } p \equiv 1 \text{ หรือ } 7 \pmod{12} \\ |\{0,1\}| = 2 & \text{เมื่อ } p \equiv 5 \text{ หรือ } 11 \pmod{12} \end{cases}$$

กรณี 1.2 $s \geq 2$ โดยทฤษฎีบทประกอบ 2.2 จะได้ว่า

$$L(n) = L(p_1^{\alpha_1})L(p_2^{\alpha_2})L(p_3^{\alpha_3}) \cdots L(p_s^{\alpha_s})$$

$$\text{ดังนั้นจากกรณี 1.1 จะได้ว่า } L(n) = 4^{\omega(n)} \cdot 2^{s-\omega(n)} = 2^{\omega(n)+s}$$

กรณี 2 $m \geq 1$

กรณี 2.1 $s = 0$ นั่นคือ $n = 2^m$ จะได้ว่า $V = \{0,1,2, \dots, 2^m - 1\}$

เนื่องจาก $2 \leq x-1 < x \leq 2^m - 1$ ทำให้ $2^m \nmid x$ และ $2^m \nmid (x-1)$

นอกจากนี้เนื่องจาก $x^2 + x + 1$ เป็นจำนวนคี่และ ห.ร.ม. ของ x และ $x-1$ เป็น 1

ดังนั้น $2^m \nmid x(x-1)(x^2 + x + 1)$ ทำให้ได้ว่า $L(2^m) = |\{0,1\}| = 2$

กรณี 2.2 $s \geq 1$ โดยทฤษฎีบทประกอบ 2.2 จะได้ว่า

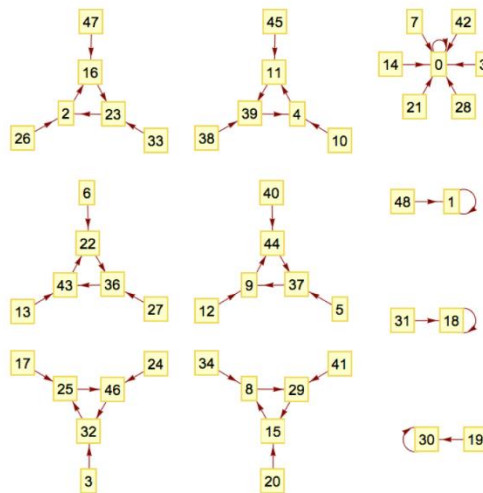
$$L(n) = L(2^m)L(p_1^{\alpha_1})L(p_2^{\alpha_2})L(p_3^{\alpha_3}) \cdots L(p_s^{\alpha_s})$$

$$\text{ดังนั้นจากกรณี 1.1 และ 2.1 จะได้ว่า } L(n) = 2 \cdot 4^{\omega(n)} \cdot 2^{s-\omega(n)} = 2^{\omega(n)+s+1}$$

□

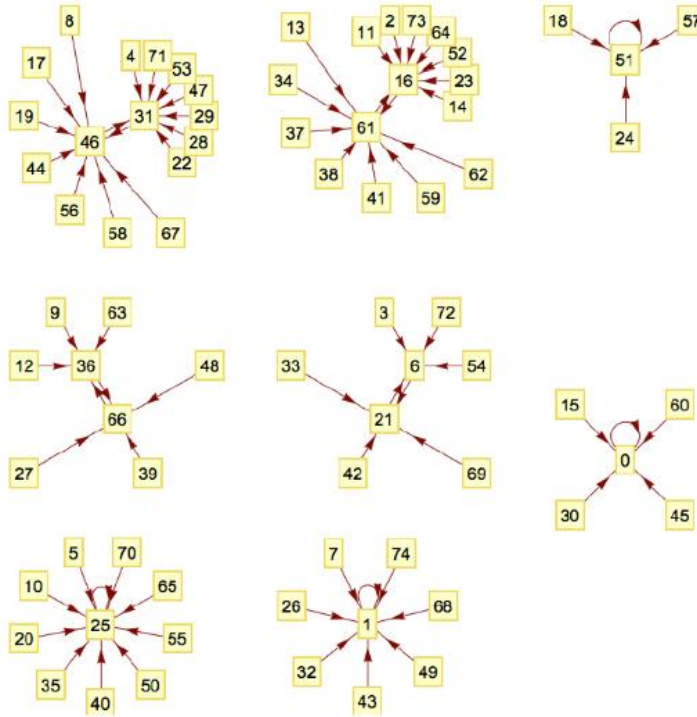
ตัวอย่าง 2.1 ให้ $n = 49$ จะได้ว่า $m = 0, s = 1$ และ $p_1 = 7 \equiv 7 \pmod{12}$

$$\text{ดังนั้น } L(49) = 2^{1+1} = 4$$



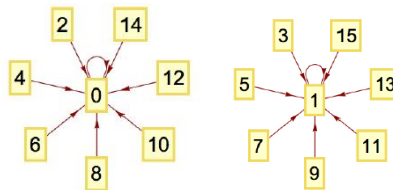
รูปที่ 2.2 $\Gamma(49,4)$

ตัวอย่าง 2.2 ให้ $n = 75$ จะได้ว่า $m = 0, s = 2, p_1 = 3 \not\equiv 1$ และ $7 \pmod{12}$ และ $p_2 = 5 \not\equiv 1$ และ $7 \pmod{12}$ ดังนั้น $\omega(75) = 0$ และ $L(75) = 2^{0+2} = 4$



รูปที่ 2.3 $\Gamma(75,4)$

ตัวอย่าง 2.3 ให้ $n = 16$ จะได้ว่า $m = 4$ และ $s = 0$ ดังนั้น $L(16) = 2^{0+0+1} = 2$



รูปที่ 2.4 $\Gamma(16,4)$

- [2] Skowronex-KaziÓw, J. (2009). Properties of Digraphs Connected with Some Congruence Relations. *Czechoslovak Mathematical Journal*, 59 (134), 39 - 49.
- [3] Ju, T. and Wu, M. (2014), On Iteration Digraph and Zero-Divisor Graph of Ring $\mathbb{Z}_n$. *Czechoslovak Mathematical Journal*, 64 (139), 39 - 49.
- [4] Somer, L. and Krížek, M. (2011), The Structure of Digraphs Associated with the Congruence $x^k \equiv y \pmod{n}$. *Czechoslovak Mathematical Journal*, 61 (136), 337 - 358.
- [5] Meemark, Y. (2016). *Theory of Numbers*. Bangkok.
- [6] อัจฉรา หาญชูวงศ์. (2542). *ทฤษฎีจำนวน*. กรุงเทพมหานคร: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.