



วารสารคณิตศาสตร์ Mathematical Journal 66(703) มกราคม – เมษายน 2564

โดย สมาคมคณิตศาสตร์แห่งประเทศไทย ในพระบรมราชูปถัมภ์

<http://www.mathassociation.net>

Email: MathThaiOrg@gmail.com

สูตรจำนวนจุดตรึงของไดกราฟที่เกิดจากความสัมพันธ์ $a^6 \equiv b \pmod{n}$

และการวางนัยทั่วไปบางแบบ

Formula for Number of Fixed Points of Digraph Arising from The Relation $a^6 \equiv b \pmod{n}$ And Some Generalization

รตินันท์ บุญเคลือบ^{1,*} และ วิภาวี คุณานพรัตน์²

¹ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

จุฬาลงกรณ์มหาวิทยาลัย กรุงเทพมหานคร 10330

²โรงเรียนเตรียมอุดมศึกษา กรุงเทพมหานคร 10330

Ratinan Boonklurb^{1,*} and Wipawee Kunanopparat²

¹Department of Mathematics and Computer Science, Faculty of Science,

Chulalongkorn University, Bangkok 10330

²Triamudomsuksa School, Bangkok 10330

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

วันที่รับบทความ : 28 กุมภาพันธ์ 2563

วันที่แก้ไขบทความ : 8 เมษายน 2563

วันที่ตอบรับบทความ : 10 พฤษภาคม 2563

บทคัดย่อ

สำหรับจำนวนนับ n ที่ $n \geq 2$ บทความฉบับนี้ให้สูตรจำนวนจุดตรึงของไดกราฟ $\Gamma(n, 6)$ ที่มีจุดยอดเป็นเซต $V = \{0, 1, 2, \dots, n-1\}$ และเส้นเชื่อมแสดงทิศทาง $(a, b) \in E \subseteq V \times V$ ก็ต่อเมื่อ

* ผู้เขียนหลัก

$a^6 \equiv b \pmod{n}$ โดยอาศัยความรู้เกี่ยวกับการแยกตัวประกอบของพหุนามไซโคลโตมิก และขยายผลไปสู่สูตรจำนวนจุดตรึงของ $\Gamma(n, k)$ เมื่อ k เป็นจำนวนนับที่ $k \geq 4$ และ $k - 1$ เป็นจำนวนเฉพาะ

คำสำคัญ: ไคกราฟ จุดตรึง พหุนามไซโคลโตมิก

ABSTRACT

For an integer n such that $n \geq 2$, this article provides a formula for number of fixed points of the digraph $\Gamma(n, 6)$ 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 $a^6 \equiv b \pmod{n}$ by using the knowledge about the factorization of the cyclotomic polynomial and extend the result to formula for number of fixed points of digraph $\Gamma(n, k)$ where k is an integer such that $k \geq 4$ and $k - 1$ is a prime number.

Keywords: Digraph, Fixed point, Cyclotomic polynomial

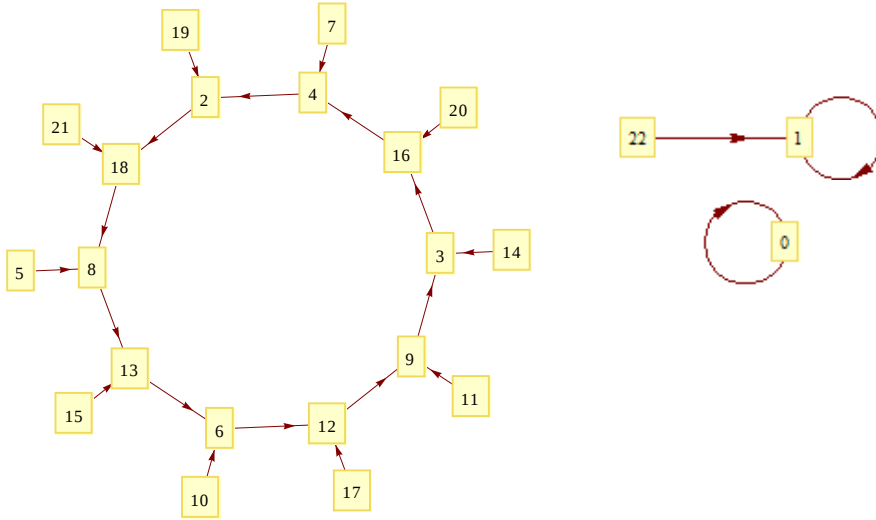
1. บทนำ

บทความฉบับนี้พิจารณาให้จำนวนนับสองจำนวนเป็นเสมือนจุดยอด แล้วนำความสัมพันธ์สมภาคระหว่างจำนวนนับสองจำนวนมาสร้างเป็นเสมือนเส้นเชื่อมระบุทิศทางระหว่างจำนวนนับทั้งสอง ซึ่งบรรดาจุดยอดและเส้นเชื่อมระบุทิศทางเหล่านี้ จะเรียกรวมกันว่า กราฟระบุทิศทาง หรือ ไคกราฟ

บทนิยาม 1.1 [6] กราฟระบุทิศทาง หรือ ไคกราฟ $G = (V, E)$ ประกอบด้วยเซตจำกัด V ที่ไม่ใช่เซตว่าง เรียกว่า เซตของจุดยอด และ E เป็นเซตของคู่อันดับที่เป็นสับเซตของ $V \times V$ โดยเรียก E ว่า เซตของเส้นเชื่อมระบุทิศทาง

ทั้งนี้ สำหรับไคกราฟ $G = (V, E)$ ถ้า $(a, b) \in E$ หมายความว่า มีเส้นเชื่อมจากจุดยอด a ไปยังจุดยอด b เรียกจุดยอด a ว่า จุดเริ่มต้น และเรียกจุดยอด b ว่า จุดปลายของเส้นเชื่อมระบุทิศทาง และมักเขียนลูกศรกำกับทิศทางไว้ ในขณะที่ถ้า $(a, a) \in E$ จะหมายถึง มีเส้นเชื่อมม้วนเป็นวงกลับมาที่จุดยอด a โดยเรียกเส้นเชื่อมลักษณะนี้ว่า วงวน และเรียกจุดยอด a ว่าเป็น จุดตรึงของไคกราฟ G นอกจากนี้ จุดยอด v ของไคกราฟ G จะเป็น จุดตรึงเอกเทศ เมื่อจุดยอด v เป็นจุดตรึงของ G ที่ไม่มีเส้นเชื่อมระบุทิศทางจากจุดยอดอื่นของ G มาเชื่อมกับจุดยอด v

ตัวอย่าง 1.1 ให้ $G = (V, E)$ โดยที่ $V = \{0, 1, 2, \dots, 22\}$ และ $E = \{(0, 0), (1, 1), (2, 18), (3, 16), (4, 2), (5, 8), (6, 12), (7, 4), (8, 13), (9, 3), (10, 6), (11, 9), (12, 9), (13, 6), (14, 3), (15, 13), (16, 4), (17, 12), (18, 8), (19, 2), (20, 16), (21, 18), (22, 1)\}$



รูปที่ 1.1 ไดกราฟ G ในตัวอย่างที่ 1.1

สังเกตว่าใน G มี $(0, 0), (1, 1) \in E$ ดังนั้น 0 และ 1 เป็นจุดตรึงของ G ซึ่งในแผนภาพจะแทนด้วยเส้นเชื่อมแสดงทิศทางที่มีลักษณะเป็นวงวนดังรูปที่ 1.1 แต่ 0 เป็นจุดตรึงเอกเทศ และ 1 ไม่เป็นจุดตรึงเอกเทศ และมี $(2, 18), (18, 8), (8, 13), (13, 6), (6, 12), (12, 9), (9, 3), (3, 16), (16, 4), (4, 2) \in E$ ซึ่งในแผนภาพแทนด้วยเส้นเชื่อมแสดงทิศทางสลับเส้นที่เชื่อมจุดยอด 2, 18, 8, 13, 6, 12, 9, 3, 16 และ 4 เข้าด้วยกันเป็นวง เรียกเส้นเชื่อมแสดงทิศทางทั้งสลับเส้นที่เชื่อมจุดยอดเหล่านี้เข้าด้วยกันว่า วง

ในปี ค.ศ.1992 นักคณิตศาสตร์ชื่อ Szalay [9] ได้สร้างไดกราฟ $\Gamma(n, 2) = (V, E)$ สำหรับจำนวนนับ n ที่ $n \geq 2$ โดยที่ $V = \{0, 1, 2, \dots, n-1\}$ และ $(a, b) \in E$ ก็ต่อเมื่อ $a^2 \equiv b \pmod{n}$ แล้วศึกษาโครงสร้างของ $\Gamma(n, 2)$ โดยเฉพาะอย่างยิ่งจำนวนจุดตรึงของ $\Gamma(n, 2)$ ต่อมา Skowronex-Kaziów [7] และ Ju และ Wu [3] ได้ศึกษาโครงสร้างและจำนวนจุดตรึงของไดกราฟลักษณะเดียวกับ Szalay [9] คือ $\Gamma(n, 3)$ และ $\Gamma(n, 5)$ โดยเปลี่ยนเงื่อนไขของการมีเส้นเชื่อมระบุทิศทาง (a, b) ในไดกราฟเป็น $a^3 \equiv b \pmod{n}$ และ $a^5 \equiv b \pmod{n}$ ตามลำดับ ในปี ค.ศ.2011 Somer และ Křížek [8] ได้ขยายแนวคิดของ Szalay [9] ศึกษาไดกราฟ $\Gamma(n, k)$ ที่เงื่อนไขการมีเส้นเชื่อมระบุ

ทิศทาง (a, b) ในไดกราฟเป็น $a^k \equiv b \pmod{n}$ เมื่อ k เป็นจำนวนนับที่ $k \geq 2$ แต่พิสูจน์ได้เพียงขอบเขตล่างของจำนวนจุดตรึงของไดกราฟ $\Gamma(n, k)$ เท่านั้น เมื่อเร็ว ๆ นี้ รตินันท์ และ ธิญพิชชา [1] ได้ให้สูตรที่เด่นชัดของจำนวนจุดตรึงของไดกราฟ $\Gamma(n, 4)$ โดยอาศัยความรู้เกี่ยวกับส่วนตกรังกำลังสอง และสัญลักษณ์ของเลขชี้กำลัง

สังเกตว่าที่ผ่านมา งานวิจัยส่วนหนึ่งมุ่งความสนใจไปที่โครงสร้างและสูตรของจำนวนจุดตรึงของ $\Gamma(n, k)$ เมื่อ k เป็นจำนวนเฉพาะ หรือจำนวนในรูปกำลังของสอง ดังนั้นในงานวิจัยนี้ จึงได้สนใจศึกษา $\Gamma(n, 6)$ ซึ่ง 6 เป็นจำนวนประกอบที่ไม่ใช่กำลังของสอง และหาสูตรที่เด่นชัดของจำนวนจุดตรึงทั้งหมดของ $\Gamma(n, 6)$ โดยอาศัยความรู้เกี่ยวกับรากปฐมฐาน ซึ่งความรู้นี้สามารถขยายไปสู่สูตรของจำนวนจุดตรึงทั้งหมดของ $\Gamma(n, k)$ เมื่อ k เป็นจำนวนนับ ที่ $k \geq 4$ และ $k - 1$ เป็นจำนวนเฉพาะ

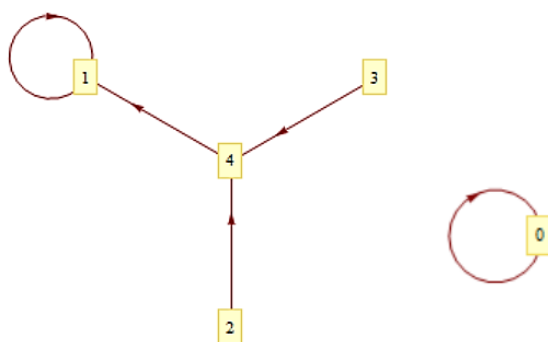
2. สูตรสำหรับจำนวนจุดตรึงของไดกราฟ $\Gamma(n, 6)$ ที่เกิดจากความสัมพันธ์ $a^6 \equiv b \pmod{n}$

ให้ n เป็นจำนวนนับ ที่ $n \geq 2$ และ $V = \{0, 1, 2, \dots, n-1\}$ นิยามไดกราฟ $\Gamma(n, 6) = (V, E)$ โดย $(a, b) \in E$ ก็ต่อเมื่อ $a^6 \equiv b \pmod{n}$

ตัวอย่าง 2.1

(i) ให้ $n = 5$

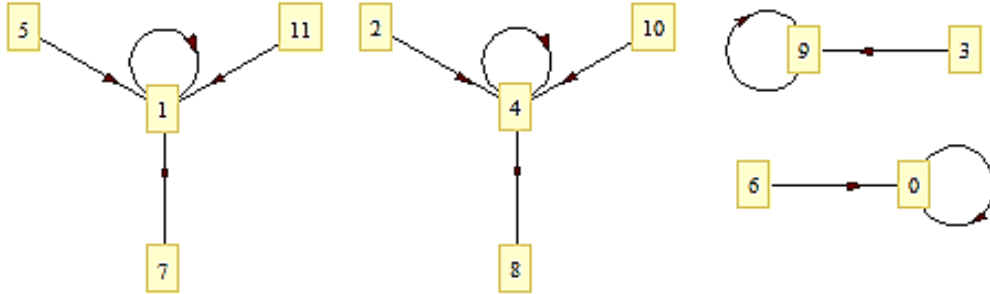
จะได้ว่า $V = \{0, 1, 2, 3, 4\}$ เนื่องจาก $0^6 \equiv 0 \pmod{5}$, $1^6 \equiv 1 \pmod{5}$, $2^6 \equiv 4 \pmod{5}$, $3^6 \equiv 4 \pmod{5}$ และ $4^6 \equiv 1 \pmod{5}$ ดังนั้น $\Gamma(5, 6)$ จะมีแผนภาพดังรูปที่ 2.1



รูปที่ 2.1 ไดกราฟ $\Gamma(5, 6)$

(ii) ให้ $n = 12$

ด้วยแนวคิดเดียวกันกับ (i) ทำให้ได้ว่า $\Gamma(12, 6)$ มีแผนภาพดังรูปที่ 2.2



รูปที่ 2.2 ไดกราฟ $\Gamma(12, 6)$

จากตัวอย่าง 2.1 จะเห็นว่า 0 เป็นจุดตรึงเอกเทศของ $\Gamma(5, 6)$ แต่ไม่เป็นจุดตรึงเอกเทศของ $\Gamma(12, 6)$ ทฤษฎีบทต่อไปจะเป็นการบอกเงื่อนไขที่จำเป็นและเพียงพอที่จะรับประกันว่าเมื่อใด 0 จะเป็นจุดตรึงเอกเทศของ $\Gamma(n, 6)$ ซึ่งเงื่อนไขและบทพิสูจน์เหมือนกับกรณี $\Gamma(n, 4)$ ที่พิสูจน์โดยดิโนนัท และธัญพิชชา [1] แต่เพื่อความสมบูรณ์ผู้เขียนขอแนะนำเสนอบทพิสูจน์ทฤษฎีบทนี้อีกครั้ง

ทฤษฎีบท 2.1 0 และ 1 เป็นจุดตรึงของ $\Gamma(n, 6)$ ยิ่งไปกว่านั้น 0 เป็นจุดตรึงเอกเทศของ $\Gamma(n, 6)$ ก็ต่อเมื่อ n ปราสจากกำลังสอง นั่นคือ n มีสมบัติว่าสำหรับจำนวนเฉพาะ p ที่เป็นตัวประกอบของ n ถ้า $p^\alpha \mid n$ แล้ว $\alpha = 1$

บทพิสูจน์ เนื่องจาก $n \mid (0^6 - 0)$ และ $n \mid (1^6 - 1)$ สำหรับทุกจำนวนนับ n จะได้ว่า 0 และ 1 เป็นจุดตรึงของ $\Gamma(n, 6)$

ต่อมาจะพิสูจน์ว่า 0 เป็นจุดตรึงเอกเทศของ $\Gamma(n, 6)$ ก็ต่อเมื่อ n ปราสจากกำลังสอง

สมมติว่า n ไม่ปราสจากกำลังสอง จะได้ว่า มีจำนวนเฉพาะ p และจำนวนเต็ม k ที่ $n = p^2 k$ จะได้ว่า $\left(\frac{n}{p}\right)^6 = n^3 k^3 \equiv 0 \pmod{n}$ ดังนั้น $\left(\frac{n}{p}, 0\right) \in E$ นั่นคือ 0 ไม่เป็นจุดตรึงเอกเทศของ $\Gamma(n, 6)$

สมมติว่า n ปราสจากกำลังสอง ทำให้ได้ว่า มีจำนวนเฉพาะ $p_1, p_2, p_3, \dots, p_l$ ซึ่งแตกต่างกันทั้งหมด ที่ $n = p_1 p_2 p_3 \dots p_l$ ต่อมาสมมติว่า 0 ไม่เป็นจุดตรึงเอกเทศ ฉะนั้นจะมี $k \in V$ และมีจำนวนเต็ม s ที่ $k^6 = p_1 p_2 p_3 \dots p_l s$ เนื่องจาก k เป็นจำนวนเต็ม ดังนั้นจะมีจำนวนเต็ม t ที่ทำให้

$$k^6 = p_1 p_2 p_3 \dots p_l (p_1 p_2 p_3 \dots p_l)^5 t^6$$

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

ข้อสังเกต 2.1 เนื่องจาก $(n-1)^6 - (n-1) = (n-1)(n^5 - 5n^4 + 10n^3 - 10n^2 + 5n - 2)$ ทำให้ได้ว่า n หาร $(n-1)^6 - (n-1)$ ลงตัว ก็ต่อเมื่อ $n = 2$ ดังนั้นสำหรับจำนวนนับ n ที่ $n \geq 3$ จุดยอด $n-1$ ไม่เป็นจุดตรึงของ $\Gamma(n, 6)$ ซึ่งเหมือนกับไดกราฟ $\Gamma(n, 4)$ ใน [1] แต่แตกต่างจากไดกราฟที่ศึกษาใน [3] และ [7] ที่ $n-1$ เป็นจุดตรึงของไดกราฟเสมอ

ต่อมาในการหาสูตรสำหรับจำนวนจุดตรึงทั้งหมดใน $\Gamma(n, 6)$ จำเป็นต้องมีความรู้พื้นฐานทางทฤษฎีจำนวนเกี่ยวกับการมีอยู่ของผลเฉลยของสมภาค $f(x) \equiv 0 \pmod{m}$

ทฤษฎีบทประกอบ 2.2 [5] (ทฤษฎีบทประกอบของเฮนเซล) ให้ $f(x)$ เป็นพหุนามในตัวแปร x ที่มีสัมประสิทธิ์เป็นจำนวนเต็ม และ 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 $i \in \{1, 2, 3, \dots, r\}$ ยิ่งไปกว่านั้น ถ้า $v(m)$ และ $v(m_i)$ เป็นจำนวนผลเฉลยของ $f(x) \equiv 0 \pmod{m}$ และ $f(x) \equiv 0 \pmod{m_i}$ ตามลำดับ แล้ว $v(m) = v(m_1)v(m_2)v(m_3) \dots v(m_r)$

นอกจากนี้ยังจำเป็นต้องทำความรู้จักกับสัญลักษณ์ การคำนวณ และบทนิยามที่เกี่ยวข้องกับทฤษฎีจำนวนเพิ่มเติมดังนี้

บทนิยาม 2.1 ให้ p เป็นจำนวนเฉพาะ

(i) [2] กำหนดให้ $\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}$ และสำหรับ $a, b \in \mathbb{Z}_p$ นิยาม

$$a \oplus b = (a + b) \pmod{p} \text{ และ } a \odot b = (ab) \pmod{p}$$

ซึ่งต่อไปจะเขียนแทน $a \oplus b$ ด้วย $a + b$ และ $a \odot b$ ด้วย ab

(ii) [2] กำหนดสัญลักษณ์ $\mathbb{Z}_p[x]$ เป็นเซตของพหุนามทั้งหมดที่มีสัมประสิทธิ์เป็นสมาชิกของ $\mathbb{Z}_p$ พร้อมการดำเนินการ $\oplus$ และ $\odot$

(iii) [4] ให้ n เป็นจำนวนนับ สมาชิก $\omega \in \mathbb{Z}_p$ จะเรียกว่าเป็น *รากที่ n ของหนึ่ง* ถ้า $\omega^n \pmod{p} = 1$ และ จะเรียกว่าเป็น *รากปฐมฐานที่ n ของหนึ่ง* ถ้า $\omega^n \pmod{p} = 1$ และ $\omega^m \pmod{p} \neq 1$ ทุกจำนวนนับ m ที่ $1 \leq m < n$

(iv) [4] ให้ n เป็นจำนวนนับ และ $\omega \in \mathbb{Z}_p$ เป็นรากปฐมฐานที่ n ของหนึ่ง นิยาม พหุนามไซโคลโตมิกอันดับที่ n เขียนแทนด้วย $\Phi_n(x)$ เป็นผลคูณในรูป

$$\Phi_n(x) = \left(\prod_{\substack{k=1 \\ \text{ห.ร.ม.}(k,n)=1}}^n (x - \omega^k) \right) \pmod{p}$$

จากบทนิยาม 2.1 (iv) จะเห็นว่า การนิยาม $\Phi_n(x)$ ขึ้นอยู่กับการมีอยู่ของรากปฐมฐานที่ n ของหนึ่งใน $\mathbb{Z}_p$

ตัวอย่าง 2.2 กำหนดให้ $p = 11$ จะได้ว่า $3^{10} \pmod{11} = 1$ ดังนั้น 3 เป็นรากที่ 10 ของหนึ่ง แต่ $3^5 \pmod{11} = 1$ และทราบว่า $3^1 \pmod{11} = 3$, $3^2 \pmod{11} = 9$, $3^3 \pmod{11} = 5$ และ $3^4 \pmod{11} = 4$ ทำให้ได้ว่า 3 ไม่เป็นรากปฐมฐานที่ 10 ของหนึ่ง แต่เป็นรากปฐมฐานที่ 5 ของหนึ่ง จึงได้ว่าพหุนามไซโคลโตมิกอันดับที่ 5 คือ

$$\begin{aligned} \Phi_5(x) &= (x - 3)(x - 3^2)(x - 3^3)(x - 3^4) \pmod{11} \\ &= (x - 3)(x - 9)(x - 5)(x - 4) \pmod{11} \\ &= (x^4 - 21x^3 + 155x^2 - 483x + 540) \pmod{11} \\ &= x^4 + x^3 + x^2 + x + 1 \end{aligned}$$

นอกจากนี้ยังสามารถตรวจสอบได้โดยง่ายว่า $10^2 \pmod{11} = 1$ และ $10 \pmod{11} = 10$ ทำให้ได้ว่า 10 เป็นรากปฐมฐานที่ 2 ของหนึ่ง จึงได้ว่าพหุนามไซโคลโตมิกอันดับที่ 2 คือ

$$\Phi_2(x) = (x - 10) \pmod{11} = x + 1$$

ในทางกลับกันเราสามารถตรวจสอบได้ว่าถ้า $a \in \mathbb{Z}_{11}$ แล้ว $a^3 \pmod{11} \neq 1$ และ $a^7 \pmod{11} \neq 1$ นั่นคือจะไม่สามารถสร้าง $\Phi_3(x)$ และ $\Phi_7(x)$ ด้วยบทนิยาม 2.1 (iv) ได้

ตัวอย่าง 2.3 กำหนดให้ $p = 7$ จะได้ว่า $2^3 \pmod{7} = 1$ และทราบว่า $2^1 \pmod{7} = 2$ และ $2^2 \pmod{7} = 4$ ทำให้ได้ว่า 2 เป็นรากปฐมฐานที่ 3 ของหนึ่ง จึงได้ว่าพหุนามไซโคลโตมิกอันดับที่ 3 คือ $\Phi_3(x) = (x - 2)(x - 2^2) \pmod{7} = (x^2 - 6x + 8) \pmod{7} = x^2 + x + 1$

จากตัวอย่างทั้งสองนี้ จะเห็นว่าสำหรับจำนวนเฉพาะ p ถ้าสามารถสร้าง $\Phi_q(x)$ เมื่อ q เป็นจำนวนเฉพาะด้วยบทนิยาม 2.1 (iv) ได้แล้ว $\Phi_q(x)$ จะมีลักษณะพิเศษกล่าวคือ

$$\Phi_q(x) = x^{q-1} + x^{q-2} + x^{q-3} + \cdots + x + 1$$

ในความเป็นจริงแล้ว $\mathbb{Z}_p$ ในบทนิยาม 2.1 (iii) และ (iv) จะสามารถแทนที่ด้วยฟิลด์ใด ๆ ก็ได้ เช่น เซตของจำนวนเชิงซ้อน ซึ่งไม่มีข้อจำกัดในการสร้าง $\Phi_n(x)$ โดยสำหรับฟิลด์ใด ๆ $\Phi_n(x)$ จะเป็นพหุนามที่มีสัมประสิทธิ์เป็นจำนวนเต็มเสมอ [4] และยังสามารถพิสูจน์ได้เช่นเดียวกันว่า สำหรับ

จำนวนเฉพาะ q ใด ๆ จะได้ว่า $\Phi_q(x) = x^{q-1} + x^{q-2} + x^{q-3} + \dots + x + 1$ ซึ่งทำให้ได้ว่าพหุนามในรูป $\Phi_q(x) = x^{q-1} + x^{q-2} + x^{q-3} + \dots + x + 1$ มองเป็นพหุนามหนึ่งใน $\mathbb{Z}_p[x]$ ได้

ดังนั้นจากตัวอย่าง 2.2 จึงอาจสามารถมองเป็นว่าพหุนาม $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ ที่สร้างจากฟีลด์ใด ๆ สามารถแยกตัวประกอบเป็นผลคูณของพหุนามเชิงเส้นใน $\mathbb{Z}_{11}[x]$ ได้ และ $\Phi_3(x) = x^2 + x + 1$ ที่สร้างจากฟีลด์ใด ๆ ไม่สามารถแยกตัวประกอบเป็นผลคูณของพหุนามเชิงเส้นใน $\mathbb{Z}_{11}[x]$ ได้ แต่สามารถแยกตัวประกอบเป็นผลคูณของพหุนามเชิงเส้นใน $\mathbb{Z}_7[x]$ ได้

ทฤษฎีบทต่อไปจะเป็นทฤษฎีบทที่รับประกันว่า เมื่อใดที่พหุนามไซโคลโตมิกซึ่งสร้างจากฟีลด์ใด ๆ จะแยกตัวประกอบเป็นผลคูณของพหุนามเชิงเส้นใน $\mathbb{Z}_p[x]$ ได้บ้าง

ทฤษฎีบทประกอบ 2.3 [4] พหุนามไซโคลโตมิก $\Phi_n(x)$ สามารถแยกตัวประกอบเป็นผลคูณของพหุนามเชิงเส้นอย่างสมบูรณ์ใน $\mathbb{Z}_p[x]$ ได้ ก็ต่อเมื่อ $p \equiv 1 \pmod{n}$

อย่างไรก็ดี ในหัวข้อที่ 2 ของบทความฉบับนี้ จะนำทฤษฎีบทประกอบ 2.3 ไปใช้ในกรณีที่ $n = 5$ และในหัวข้อที่ 3 จึงจะนำทฤษฎีบทประกอบ 2.3 ไปใช้ในกรณีทั่วไปยิ่งขึ้น

ต่อไปจะเป็นการนำทฤษฎีบทประกอบต่าง ๆ ข้างต้นมาช่วยในการพิสูจน์ทฤษฎีบทหลักเกี่ยวกับจำนวนจุดตรึงทั้งหมดของ $\Gamma(n, 6)$

ทฤษฎีบท 2.4 ให้ s และ n เป็นจำนวนนับ โดยที่ $n \geq 2$ และ n แยกตัวประกอบได้ในรูป

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$$

โดย $p_1 < p_2 < p_3 < \dots < p_s$ เป็นจำนวนเฉพาะ α_i เป็นจำนวนเต็มที่ไม่เป็นลบและไม่เป็นศูนย์พร้อมกันทั้งหมด ถ้า $\pi(n)$ แทนจำนวนของจำนวนเฉพาะ p_i ที่แตกต่างกันทั้งหมดที่เป็นตัวประกอบของ n ซึ่ง $p_i \equiv 1 \pmod{5}$ แล้วจำนวนจุดตรึงทั้งหมดใน $\Gamma(n, 6)$ คือ $2^s 3^{\pi(n)}$ จุด

บทพิสูจน์ กำหนดให้ $L(n)$ เป็นจำนวนจุดตรึงทั้งหมดใน $\Gamma(n, 6)$ ดังนั้น $L(n)$ เป็นจำนวนผลเฉลี่ยใน $V = \{0, 1, 2, \dots, n-1\}$ ของสมภาค

$$f(x) = x^6 - x = x(x-1)(x^4 + x^3 + x^2 + x + 1) \equiv 0 \pmod{n}$$

กรณี 1 $s = 1$

โดยไม่เสียไรทั่วไปให้ $n = p^\alpha$ เมื่อ p เป็นจำนวนเฉพาะและ α เป็นจำนวนนับ

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

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

เนื่องจาก $p \mid p^\alpha$ ทำให้ได้ว่า $p \mid x$ หรือ $p \mid (x - 1)$ หรือ $p \mid (x^4 + x^3 + x^2 + x + 1)$

กรณี 1.1 $p \mid x$

สมมติว่า $p \mid (x - 1)$ หรือ $p \mid (x^4 + x^3 + x^2 + x + 1)$ จะได้ว่า $p \mid 1$ ทำให้เกิดข้อขัดแย้ง
 ดังนั้น $p \nmid (x - 1)$ และ $p \nmid (x^4 + x^3 + x^2 + x + 1)$ ทำให้ได้ว่า $p^\alpha \nmid (x - 1)$ และ
 $p^\alpha \nmid (x^4 + x^3 + x^2 + x + 1)$ และเนื่องจาก $2 \leq x \leq p^\alpha - 1$ ทำให้ได้ว่า $p^\alpha \nmid x$ เช่นกัน
 ดังนั้นกรณี 1.1 นี้ไม่เกิดขึ้น

กรณี 1.2 $p \mid (x - 1)$

สมมติว่า $p \mid x$ จะได้ว่า $p \mid 1$ ทำให้เกิดข้อขัดแย้ง

ต่อมา สมมติว่า $p \mid (x^4 + x^3 + x^2 + x + 1)$ เนื่องจาก $p \mid (x - 1)$ จะได้ว่ามีจำนวนเต็ม t ที่
 $x = pt + 1$ ทำให้ได้ว่า

$$\begin{aligned} x^4 + x^3 + x^2 + x + 1 &= (pt + 1)^4 + (pt + 1)^3 + (pt + 1)^2 + (pt + 1) + 1 \\ &\equiv 1 + 1 + 1 + 1 + 1 = 5 \pmod{p} \end{aligned}$$

แต่ $p \mid (x^4 + x^3 + x^2 + x + 1)$ จึงทำให้ $p \mid 5$ ดังนั้น $p = 5$ นั่นคือ $p \mid (x^4 + x^3 + x^2 + x + 1)$
 ทำให้เกิดสมภาค $x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{5}$ เมื่อ $x \neq 0$ และ 1 อย่างไรก็ตามเมื่อคำนวณ
 โดยตรงพบว่า

$$\begin{aligned} 2^4 + 2^3 + 2^2 + 2 + 1 &= 31 \not\equiv 0 \pmod{5} \\ 3^4 + 3^3 + 3^2 + 3 + 1 &= 121 \not\equiv 0 \pmod{5} \\ 4^4 + 4^3 + 4^2 + 4 + 1 &= 341 \not\equiv 0 \pmod{5} \end{aligned}$$

จึงทำให้เกิดข้อขัดแย้ง ทำให้ได้ว่า $p \nmid x$ และ $p \nmid (x^4 + x^3 + x^2 + x + 1)$ จึงได้ว่า $p^\alpha \nmid x$
 และ $p^\alpha \nmid (x^4 + x^3 + x^2 + x + 1)$ และเนื่องจาก $1 \leq x - 1 \leq p^\alpha - 2$ ทำให้ได้ว่า $p^\alpha \nmid x - 1$
 เช่นกัน ดังนั้นกรณี 1.2 นี้ไม่เกิดขึ้น

กรณี 1.3 $p \mid (x^4 + x^3 + x^2 + x + 1)$

นั่นคือสมภาค $x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{p}$ สังเกตว่า $x^4 + x^3 + x^2 + x + 1$ คือ
 $\Phi_5(x)$ และโดยทฤษฎีบทประกอบ 2.3 จะได้ว่า $\Phi_5(x)$ แยกตัวประกอบได้เป็นผลคูณของพหุนาม
 เชิงเส้นอย่างสมบูรณ์ 4 พหุนามได้ใน $\mathbb{Z}_p[x]$ ได้ ก็ต่อเมื่อ $p \equiv 1 \pmod{5}$

ดังนั้นสมภาคในกรณีย่อยนี้มีผลเฉลย 4 ตัว สมมติว่าเป็น a, b, c และ d ก็ต่อเมื่อ $p \equiv 1 \pmod{5}$
 จากทฤษฎีบท 2.1 และ กรณี 1.1, 1.2 และ 1.3 จะได้ว่า

$$L(n) = \begin{cases} |\{0, 1, a, b, c, d\}| = 6 & \text{เมื่อ } p \equiv 1 \pmod{5} \\ |\{0, 1\}| = 2 & \text{เมื่อ } p \not\equiv 1 \pmod{5} \end{cases}$$

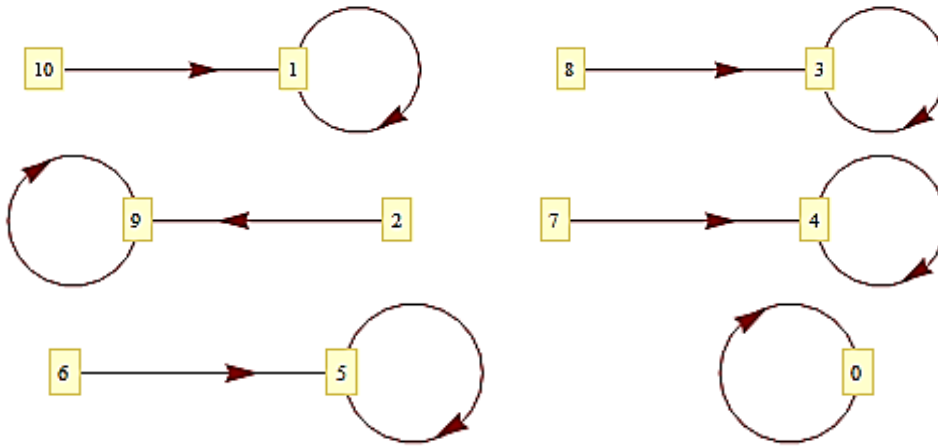
กรณี $2 \leq s$

โดยทฤษฎีบทประกอบ 2.2 จะได้ว่า

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

ดังนั้นจากกรณี 1 จะได้ว่า $L(n) = 6^{\pi(n)} \cdot 2^{s-\pi(n)} = 2^s 3^{\pi(n)}$ □

ตัวอย่าง 2.3 ให้ $n = 11$ หรือ $n = 31$ จะได้ว่า $s = 1$ และ $p_1 = 11 \equiv 1 \pmod{5}$ หรือ $p_1 = 31 \equiv 1 \pmod{5}$ ดังนั้น $\pi(11) = \pi(31) = 1$ และ $L(11) = 2^1 3^1 = 6$



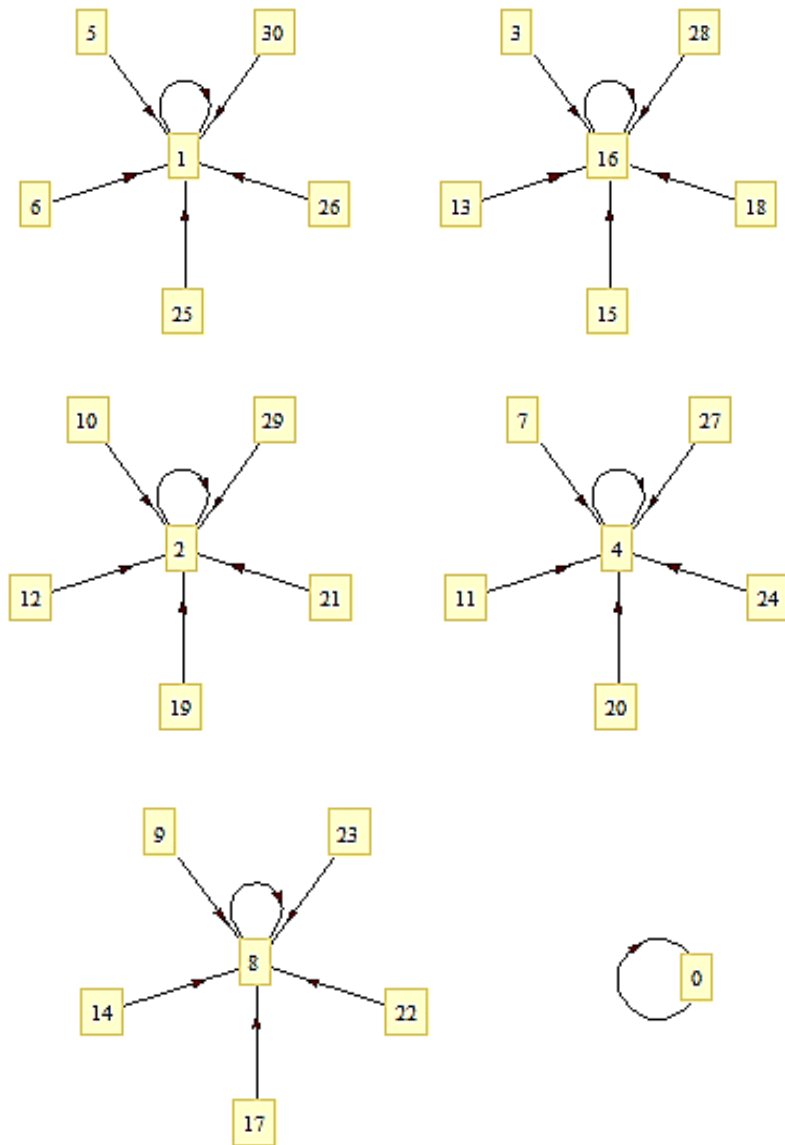
รูปที่ 2.3 ไคกราฟ $\Gamma(11, 6)$

ข้อสังเกต 2.2 (i) ใน $\mathbb{Z}_{11}$ จากตัวอย่าง 2.2 ทำให้ทราบว่า 3 เป็นรากปฐมฐานที่ 5 ของหนึ่ง และสังเกตจากรูปที่ 2.3 ได้ว่า $3^1 \pmod{11} = 3$, $3^2 \pmod{11} = 9$, $3^3 \pmod{11} = 5$ และ $3^4 \pmod{11} = 4$ เป็น 4 จุดตรึงในบรรดา 6 จุดตรึงทั้งหมดของ $\Gamma(11, 6)$

(ii) ในทำนองเดียวกัน ใน $\mathbb{Z}_{31}$ สามารถตรวจสอบได้ว่า 2 เป็นรากปฐมฐานที่ 5 ของหนึ่ง และสังเกตจากรูปที่ 2.4 ได้ว่า $2^1 \pmod{31} = 2$, $2^2 \pmod{31} = 4$, $2^3 \pmod{31} = 8$ และ $2^4 \pmod{31} = 16$ เป็น 4 จุดตรึงในบรรดา 6 จุดตรึงทั้งหมดของ $\Gamma(31, 6)$

ดังนั้นโดยบทนิยามของรากปฐมฐานที่ 5 ของหนึ่ง บทนิยามของ $\Phi_5(x)$ และข้อสังเกต 2.2 ทำให้ได้บทแทรกดังต่อไปนี้

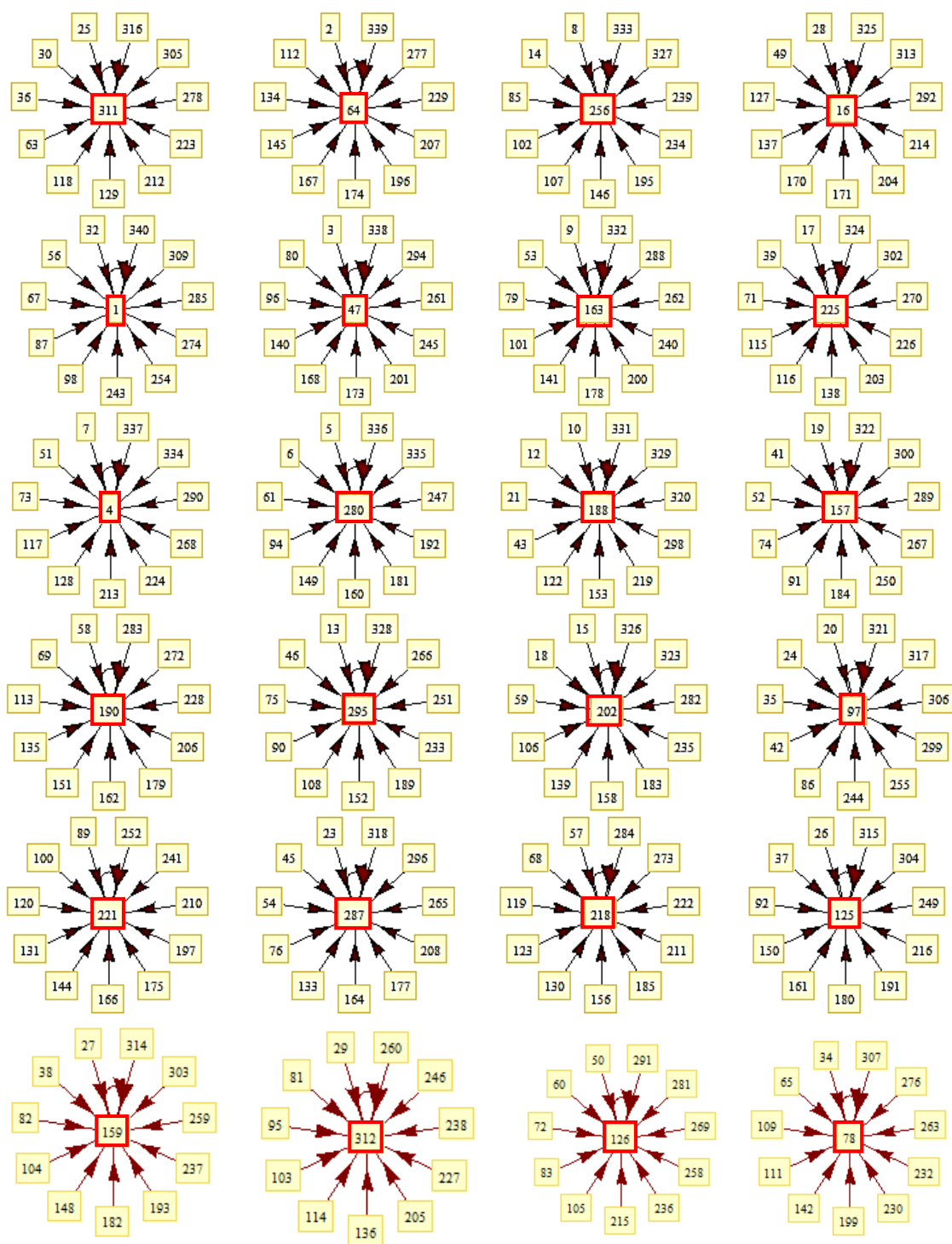
บทแทรก 2.5 ให้ p เป็นจำนวนเฉพาะที่ $p \equiv 1 \pmod{5}$ และ ω เป็นรากปฐมฐานที่ 5 ของหนึ่งใน $\mathbb{Z}_p$ จะได้ว่า $\Gamma(p, 6)$ มีจุดตรึง 6 จุด ได้แก่ 0 , 1 , $\omega \pmod{p}$, $\omega^2 \pmod{p}$, $\omega^3 \pmod{p}$ และ $\omega^4 \pmod{p}$



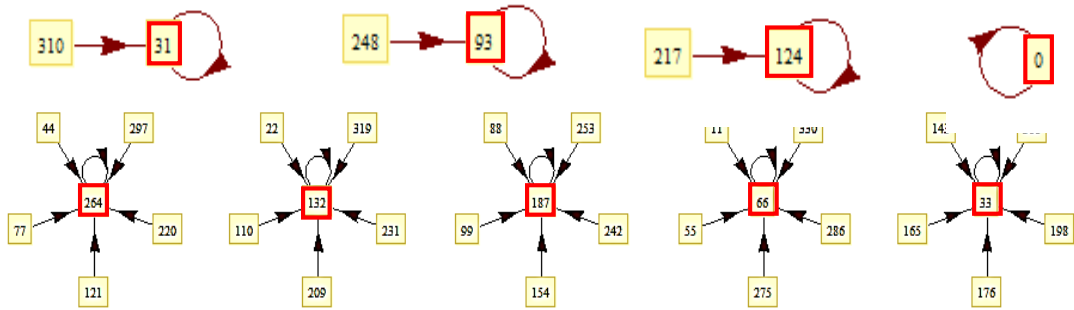
รูปที่ 2.4 ไดกราฟ $\Gamma(31, 6)$

ตัวอย่าง 2.4 ให้ $n = 341$ จะได้ว่า $s = 2$, $p_1 = 11 \equiv 1 \pmod{5}$ และ $p_2 = 31 \equiv 1 \pmod{5}$

ดังนั้น $\pi(341) = 2$ และ $L(341) = 2^2 3^2 = 36$



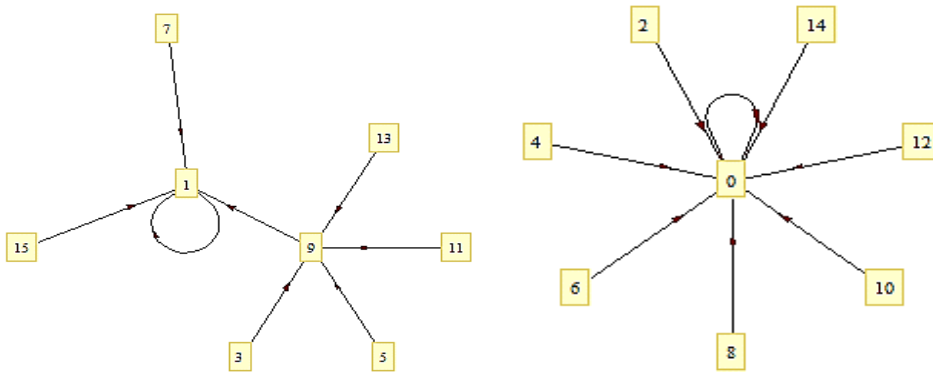
รูปที่ 2.5 ไดกราฟ $\Gamma(341, 6)$



รูปที่ 2.5 (ต่อ) ไดกราฟ $\Gamma(341, 6)$

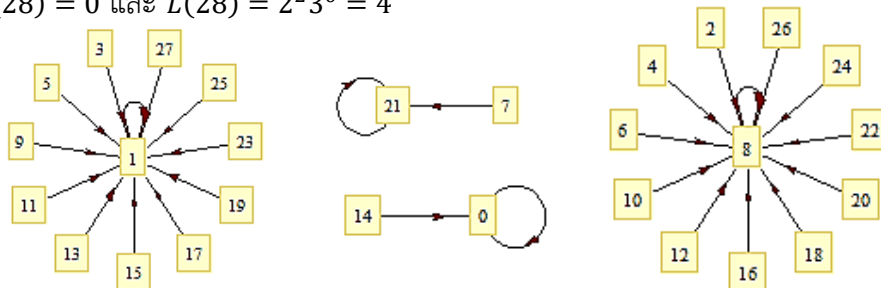
หมายเหตุ เนื่องจากข้อจำกัดของโปรแกรมสำเร็จรูปที่ใช้ในการสร้างแผนภาพ ในที่นี้ขอใช้กรอบหนาเพื่อเน้นจุดที่มีวงวน

ตัวอย่าง 2.3 ให้ $n = 16$ จะได้ว่า $s = 1$ และ $p_1 = 2 \not\equiv 1 \pmod{5}$ ดังนั้น $\pi(16) = 0$ และ $L(16) = 2^1 3^0 = 2$



รูปที่ 2.6 ไดกราฟ $\Gamma(16, 6)$

ตัวอย่าง 2.4 ให้ $n = 28$ จะได้ว่า $s = 2$, $p_1 = 2 \not\equiv 1 \pmod{5}$ และ $p_2 = 7 \not\equiv 1 \pmod{5}$ ดังนั้น $\pi(28) = 0$ และ $L(28) = 2^2 3^0 = 4$



รูปที่ 2.7 ไดกราฟ $\Gamma(28, 6)$

3. การวางนัยทั่วไป

ดังที่ได้กล่าวมาแล้วในหัวข้อที่ 2 ว่า Kanoksing [4] สามารถพิสูจน์ได้ว่า ถ้า q เป็นจำนวนเฉพาะใด ๆ แล้ว สำหรับฟิลด์ใด ๆ

$$\Phi_q(x) = x^{q-1} + x^{q-2} + x^{q-3} + \cdots + x + 1$$

และสำหรับจำนวนเต็ม k ที่ $k \geq 4$ สมภาคที่เกี่ยวข้องกับการหาจำนวนจุดตรึงของ $\Gamma(n, k)$ คือ

$$x^k - x = x(x-1)(x^{k-2} + x^{k-3} + x^{k-4} + \cdots + x + 1) \equiv 0 \pmod{n}$$

ซึ่งจะได้ว่า เมื่อ $k-1$ เป็นจำนวนเฉพาะ แล้ว $\Phi_{k-1}(x) = x^{k-2} + x^{k-3} + x^{k-4} + \cdots + x + 1$

ต่อมาเมื่อพิจารณาบทพิสูจน์ของทฤษฎีบท 2.4 กรณีที่ 1.3 จะพบว่า โดยทฤษฎีบทประกอบ 2.3 จะได้ว่า $\Phi_{k-1}(x) \equiv 0 \pmod{p}$ จะแยกตัวประกอบเป็นผลคูณของพหุนามเชิงเส้น $k-2$ ตัว อย่างสมบูรณ์ได้ใน $\mathbb{Z}_p[x]$ และมีผลเฉลย $k-2$ ตัว ก็ต่อเมื่อ $p \equiv 1 \pmod{k-1}$ จึงสามารถวางนัยทั่วไปของทฤษฎีบท 2.4 และบทแทรก 2.5 ได้เป็น

ทฤษฎีบท 3.1 ให้ s และ n เป็นจำนวนนับที่ $n \geq 2$ ซึ่งแยกตัวประกอบได้ในรูป

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

โดย $p_1 < p_2 < p_3 < \cdots < p_s$ เป็นจำนวนเฉพาะ α_i เป็นจำนวนเต็มที่ไม่เป็นลบและไม่เป็นศูนย์ พร้อมกันทั้งหมด ถ้า k เป็นจำนวนนับที่ $k \geq 4$ และ $k-1$ เป็นจำนวนเฉพาะ แล้วจำนวนจุดตรึงทั้งหมดใน $\Gamma(n, k)$ คือ $k^{\pi(n)} 2^{s-\pi(n)}$ จุด เมื่อ $\pi(n)$ แทนจำนวนของจำนวนเฉพาะ p_i ที่แตกต่างกันทั้งหมดที่เป็นตัวประกอบของ n ซึ่ง $p_i \equiv 1 \pmod{k-1}$

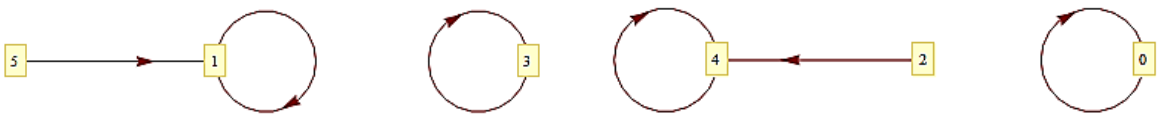
บทแทรก 3.2 ให้ k เป็นจำนวนนับที่ $k \geq 4$ และ $k-1$ เป็นจำนวนเฉพาะ และ p เป็นจำนวนเฉพาะที่ $p \equiv 1 \pmod{k-1}$ ถ้า ω เป็นรากปฐมฐานที่ $k-1$ ของหนึ่งใน $\mathbb{Z}_p$ จะได้ว่า $\Gamma(p, k)$ มีจุดตรึง k จุด ได้แก่ $0, 1, \omega \pmod{p}, \omega^2 \pmod{p}, \omega^3 \pmod{p}, \dots, \omega^{k-2} \pmod{p}$

ตัวอย่าง 3.1 ให้ $k = 4$ จะได้ว่า $k-1 = 3$ เป็นจำนวนเฉพาะ ดังนั้นจำนวนจุดตรึงทั้งหมดใน $\Gamma(n, 4)$ คือ $4^{\pi(n)} 2^{s-\pi(n)} = 2^{\pi(n)+s}$ จุด เมื่อ $\pi(n)$ แทนจำนวนของจำนวนเฉพาะ p_i ที่เป็นตัวประกอบของ n ซึ่ง $p_i \equiv 1 \pmod{3}$

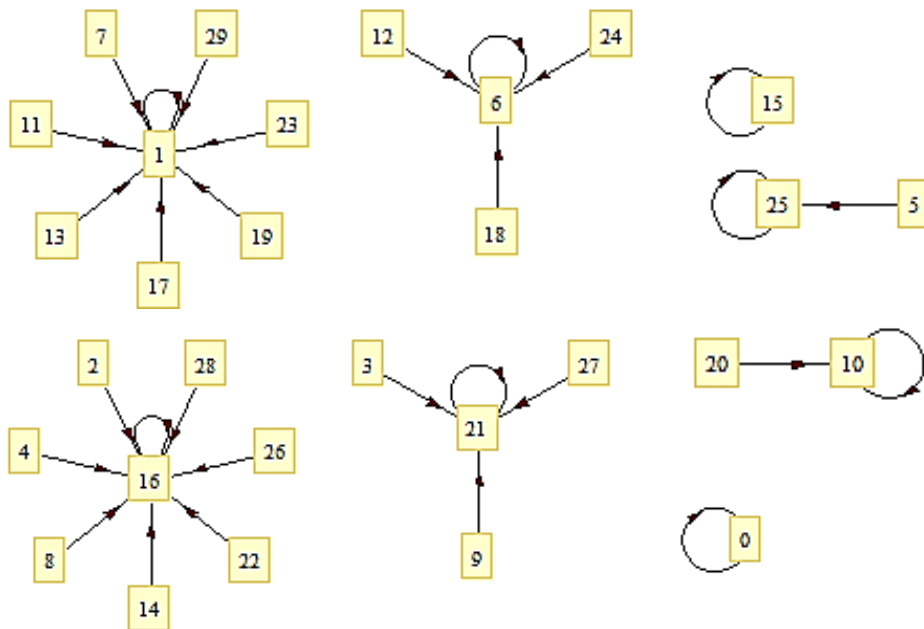
สังเกตว่าสำหรับจำนวนเฉพาะ p_i จะได้ว่า ถ้า $p_i = 2$ แล้ว $p_i \not\equiv 1 \pmod{3}$ และ $p_i \equiv 1 \pmod{3}$ ก็ต่อเมื่อ $p_i \equiv 1 \pmod{12}$ หรือ $p_i \equiv 7 \pmod{12}$ ทำให้จำนวนของจำนวนเฉพาะ p_i ที่เป็นตัวประกอบของ n ซึ่ง $p_i \equiv 1 \pmod{3}$ และจำนวนของจำนวนเฉพาะ p_i ที่เป็นตัว

ประกอบของ n ซึ่ง $p_i = 2$ หรือ $p_i \equiv 1 \pmod{12}$ หรือ $p_i \equiv 7 \pmod{12}$ มีจำนวนเท่ากัน ซึ่งสูตรจำนวนจุดตรึงในตัวอย่างนี้ตรงกับสูตรจำนวนจุดตรึงทั้งหมดใน $\Gamma(n, 4)$ ที่นำเสนอใน [1]

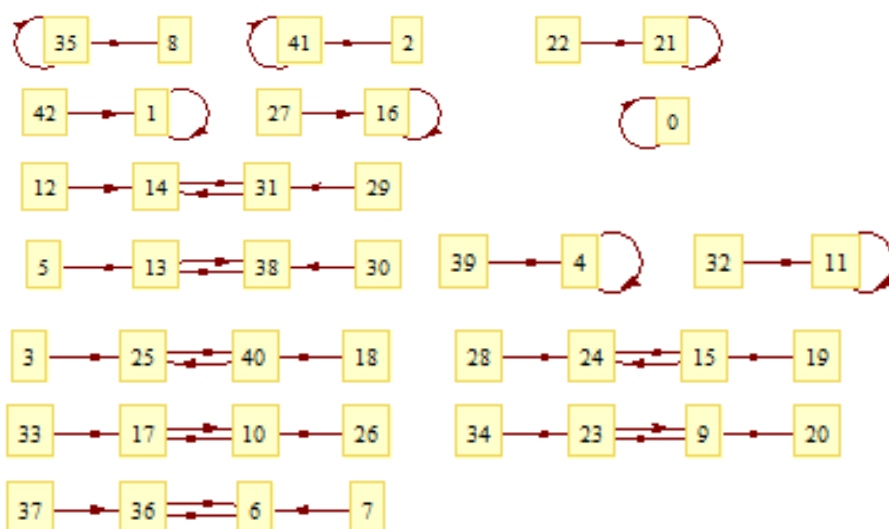
ตัวอย่าง 3.2 ให้ $k = 8$ จะได้ว่า $k - 1 = 7$ เป็นจำนวนเฉพาะ ดังนั้น จำนวนจุดตรึงทั้งหมดใน $\Gamma(n, 8)$ คือ $8^{\pi(n)} 2^{s-\pi(n)} = 2^{2\pi(n)+s}$ จุด เมื่อ $\pi(n)$ แทนจำนวนของจำนวนเฉพาะ p_i ที่เป็นตัวประกอบของ n ซึ่ง $p_i \equiv 1 \pmod{7}$ รูปที่ 3.1 3.2 และ 3.3 เป็นแผนภาพของ $\Gamma(6, 8)$, $\Gamma(30, 8)$ และ $\Gamma(43, 8)$ ซึ่งมีจุดตรึง 4, 8 และ 8 จุด ตามลำดับ สังเกตว่า 4 เป็นรากปฐมฐานที่ 7 ของ 1 ใน $\mathbb{Z}_{43}$ จึงได้ว่า $4 \pmod{43} = 4$, $4^2 \pmod{43} = 16$, $4^3 \pmod{43} = 21$, $4^4 \pmod{43} = 41$, $4^5 \pmod{43} = 35$ และ $4^6 \pmod{43} = 11$ เป็นจุดตรึง 6 จุด ในบรรดา 8 จุดของ $\Gamma(43, 8)$



รูปที่ 3.1 ไดกราฟ $\Gamma(6, 8)$

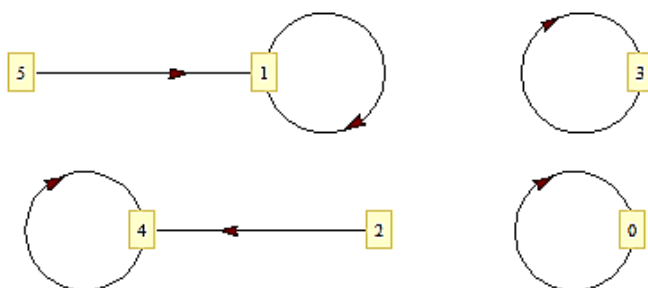


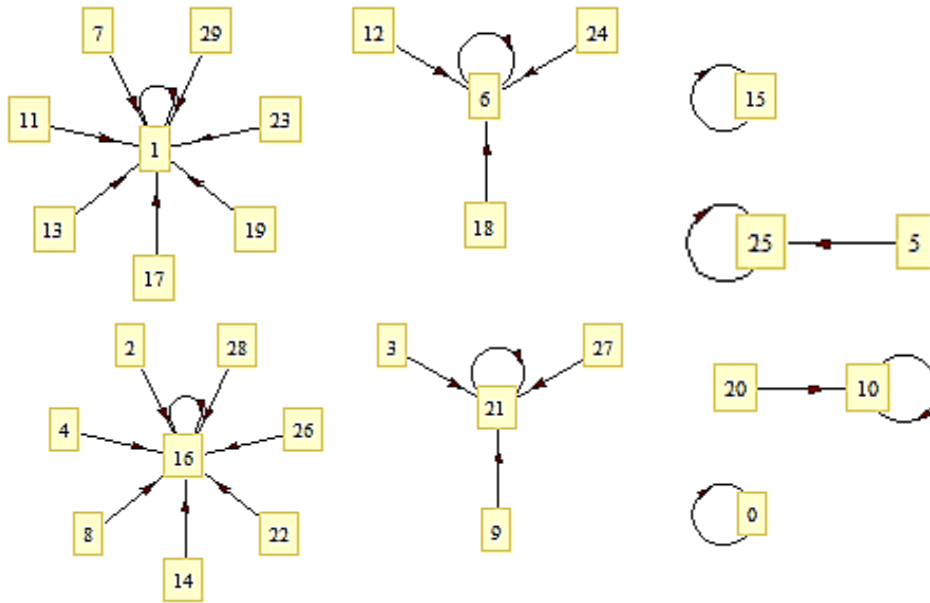
รูปที่ 3.2 ไดกราฟ $\Gamma(30, 8)$

รูปที่ 3.3 ไคกราฟ $\Gamma(43, 8)$

ตัวอย่าง 3.3 ให้ $k = 12$ จะได้ว่า $k - 1 = 11$ เป็นจำนวนเฉพาะ ดังนั้น จำนวนจุดตรึงทั้งหมดใน $\Gamma(n, 12)$ คือ $12^{\pi(n)} 2^{s-\pi(n)} = 2^{\pi(n)+s} 3^{\pi(n)}$ จุด เมื่อ $\pi(n)$ แทนจำนวนของจำนวนเฉพาะ p_i ที่เป็นตัวประกอบของ n ซึ่ง $p_i \equiv 1 \pmod{11}$ รูปที่ 3.4 3.5 และ 3.6 เป็นแผนภาพของ $\Gamma(6, 12)$, $\Gamma(30, 12)$ และ $\Gamma(67, 12)$ ซึ่งมีจุดตรึง 4, 8 และ 12 จุด ตามลำดับ

สังเกตว่า 9 เป็นรากปฐมฐานที่ 11 ของ 1 ใน $\mathbb{Z}_{67}$ จึงได้ว่า $9 \pmod{67} = 9$, $9^2 \pmod{67} = 14$, $9^3 \pmod{67} = 59$, $9^4 \pmod{67} = 62$, $9^5 \pmod{67} = 22$, $9^6 \pmod{67} = 64$, $9^7 \pmod{67} = 40$, $9^8 \pmod{67} = 25$, $9^9 \pmod{67} = 24$ และ $9^{10} \pmod{67} = 15$ เป็นจุดตรึง 10 จุด ในบรรดา 12 จุดของ $\Gamma(67, 12)$

รูปที่ 3.4 ไคกราฟ $\Gamma(6, 12)$



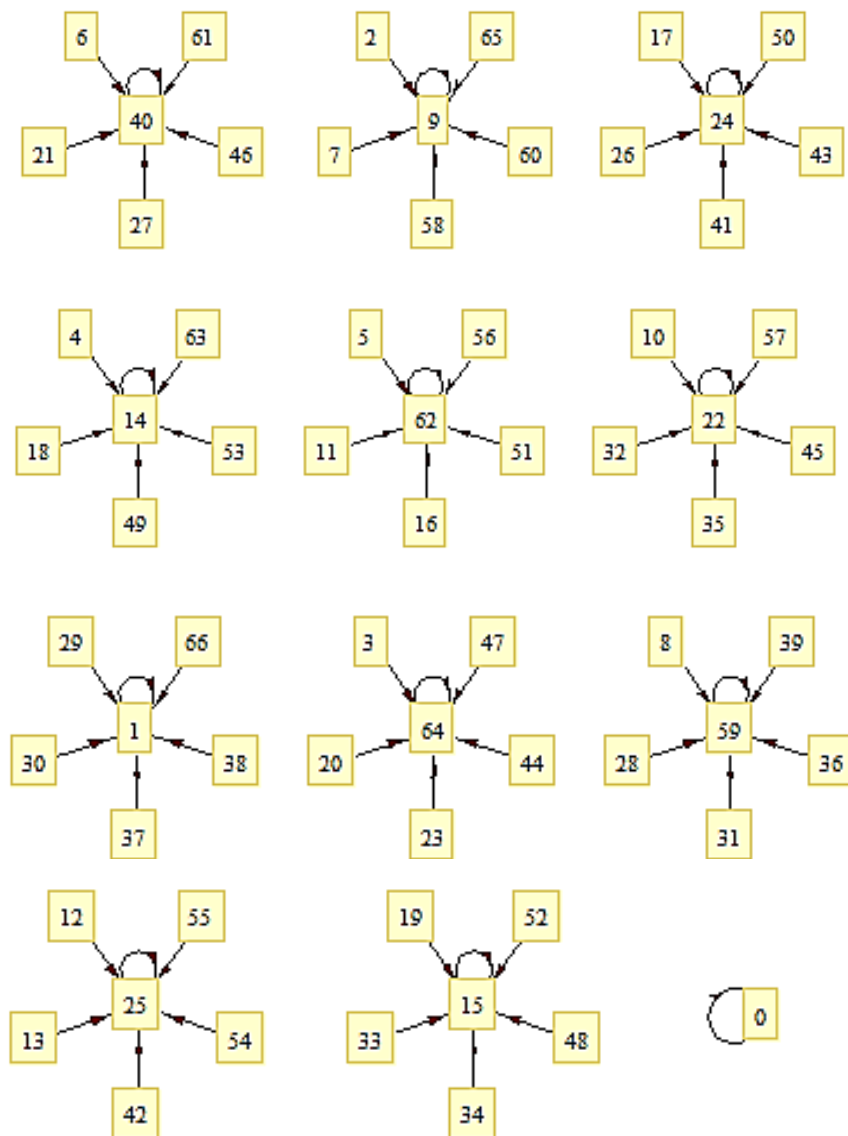
รูปที่ 3.5 ไดรกราฟ $\Gamma(30, 12)$

ในกรณีที่ $k = 3$ จริงอยู่ที่ว่า $k - 1 = 2$ เป็นจำนวนเฉพาะ แต่ $\Phi_2(x) = x + 1$ ซึ่งเป็นพหุนามเชิงเส้นอยู่แล้ว และจำนวนผลเฉลยของสมภาคที่เกี่ยวข้องกับการหาจำนวนจุดตรึงของ $\Gamma(n, 3)$ ซึ่งคือ $x^3 - x = x(x - 1)(x + 1) \equiv 0 \pmod{n}$ ขึ้นอยู่กับกำลังของ 2 ที่เป็นตัวประกอบของ n ทำให้สูตรของจำนวนจุดตรึงของ $\Gamma(n, 3)$ แตกต่างจากทฤษฎีบท 3.1 ซึ่งผู้ที่สนใจสามารถอ่านเพิ่มเติมได้ใน [6]

จะเห็นว่าการนำความรู้เกี่ยวกับการแยกตัวประกอบของพหุนามไซโคลโตมิกมาร่วมพิจารณาช่วยให้การหาสูตรจำนวนจุดตรึงของ $\Gamma(n, 6)$ ทำได้ง่ายขึ้น และยังขยายผลไปได้ยังกรณีที่ทั่วไปกว่าได้ด้วย สำหรับผู้ที่สนใจอาจศึกษาเพิ่มเติมว่า จุดยอดใดบ้างจะเป็นจุดตรึงของ $\Gamma(n, 6)$ เมื่อ n เป็นจำนวนนับที่ $n \geq 2$ จุดยอดเหล่านี้มีความเกี่ยวข้องกับรากปฐมฐานหรือไม่ อย่างไร และสามารถขยายผลนี้ไปยังกรณีที่ทั่วไปกว่าได้หรือไม่

กิตติกรรมประกาศ

งานวิจัยนี้เป็นส่วนหนึ่งของโครงการคณิตศาสตร์ที่ได้รับการสนับสนุนโดยทุนพัฒนาและส่งเสริมผู้มีความสามารถพิเศษทางวิทยาศาสตร์และเทคโนโลยี (พสวท.)



รูปที่ 3.6 ไดกราฟ $\Gamma(67, 12)$

เอกสารอ้างอิง

- [1] รตินันท์ บุญเคลือบ และ ัญพิชชา ยอดแก้ว. (2561). ไดกราฟที่เกิดจากความสัมพันธ์ $a^4 \equiv b \pmod{n}$. *วารสารคณิตศาสตร์ โดยสมาคมคณิตศาสตร์แห่งประเทศไทย ในพระบรมราชูปถัมภ์*, 63 (695), น. 9 - 18.
Boonklurb, R. and Yodkeaw, T. (2018). Digraph Arising from The Relation $a^4 \equiv b \pmod{n}$. *Mathematical Journal by The Mathematical Association of Thailand under The Patronage of His Majesty the King*, 63 (695), p. 9 - 18.
- [2] อัจฉรา หาญชูวงศ์. (2542). *ทฤษฎีจำนวน*. กรุงเทพมหานคร: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.
Harnchoowong, A. (1999). *Theory of Numbers*. Bangkok: Chulalongkorn University Printery.
- [3] Ju, T. and Wu, M. (2014). On Iteration Digraph and Zero-Divisor Graph of Ring $\mathbb{Z}_n$. *Czechoslovak Mathematical Journal*, 64 (139), p. 611 - 628.
- [4] Kanoksing, P. (2017). *Structure of The Quotient Ring of Polynomials over Integer Modulo m with The n^{th} Cyclotomic Polynomial*. (Senior Project). Chulalongkorn University, Faculty of Science, Department of Mathematics and Computer Science.
- [5] Meemark, Y. (2016). *Theory of Numbers*. Retrieved from <http://pioneer.netserv.chula.ac.th/~myotsana/MATH331NT.pdf>.
- [6] Rosen, K. H. (1999). *Discrete Mathematics and Its Applications* (4th ed.). McGraw-Hill International Edition.
- [7] Skowronex-Kaziów, J. (2009). Properties of Digraphs Connected with Some Congruence Relations. *Czechoslovak Mathematical Journal*, 59 (134), p. 39 - 49.
- [8] Somer, L. and Křížek, M. (2011). The Structure of Digraphs Associated with the Congruence $x^k \equiv y \pmod{n}$. *Czechoslovak Mathematical Journal*, 61 (136), p. 337 - 358.

- [9] Szalay, L. (1992). A Discrete Iteration in Number Theory. *BDTF Tud. Közl.*, 8, p. 71 - 91 (in Hungarian).