สับเซตของเซต $\{1,2,\ldots,2n\}$ ที่มีสมาชิก n ตัวและผลบวกของสมาชิกหารด้วย n ลงตัว

นางสาวศิริญญา โปร่งจิตร์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์

คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2544

ISBN 974-17-0127-6

n-ELEMENT SUBSETS OF $\{1,2,\ldots,2n\}$ WHOSE SUMS ARE DIVISIBLE BY n

Miss Sirinya Prongjit

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science in Mathematics

Department of Mathematics

Faculty of Science

Chulalongkorn University

Academic Year 2001

ISBN 974-17-0127-6

หัวข้อวิทยานิพนธ์	สับเซตของเซต $\{1,2,\ldots,2n\}$ ที่มีสมาชิก n ตัวและผลบวกของสมาชิกหารด้วย n ลงตัว
โดย	นางสาวศิริญญา โปร่งจิตร์
สาขาวิชา	คณิตศาสตร์
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์ ดร. พัฒนี อุดมกะวานิช

คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.... รองคณบดีฝ่ายบริหาร
(รองศาสตราจารย์ ดร. พิพัฒน์ การเที่ยง) รักษาราชการแทนคณบดี
คณะวิทยาศาสตร์

คณะกรรมการสอบวิทยานิพนธ์

....ประธานกรรมการ
(รองศาสตราจารย์ ดร. วนิดา เหมะกุล)

....อาจารย์ที่ปรึกษา
(ผู้ช่วยศาสตราจารย์ ดร. พัฒนี อุดมกะวานิช)

....กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. อัจฉรา หาญชูวงศ์)

ศิริญญา โปร่งจิตร์ : สับเซตของเซต $\{1,2,\ldots,2n\}$ ที่มีสมาชิก n ตัวและผลบวกของสมาชิกหารด้วย n ลงตัว. (n-ELEMENT SUBSETS OF $\{1,2,\ldots,2n\}$ WHOSE SUMS ARE DIVISIBLE BY n) อ. ที่ปรึกษา : ผู้ช่วยศาสตราจารย์ ดร.พัฒนี อุดมกะวานิช, 33 หน้า. ISBN 974-17-0127-6.

ในงานวิจัยนี้ เราสนใจโจทย์ปัญหาข้อ 6 ในการแข่งขันคณิตศาสตร์โอลิมปิกระหว่างประเทศในปี พ.ศ. 2538 ที่กล่าวว่า

" ให้ p เป็นจำนวนเฉพาะคี่ใด ๆ จงหาจำนวนของสับเซต A ของเซต $\{1,2,\ldots,2p\}$ ซึ่งมีสมบัติว่า

(1) A มีสมาชิก p ตัว และ

(2) ผลบวกของสมาชิกใน A หารด้วย p ลงตัว "

โจทย์ข้อนี้มีวิธีหาผลเฉลยได้อย่างน้อย 3 วิธี เราเสนอวิธีที่ 4 โดยการใช้การกระทำของกรุปบนเซต นอกจากนี้ เราได้ขยายขอบเขตของปัญหาศึกษากรณีจำนวนเต็มบวก n ใด ๆ แทนที่จะเป็นจำนวนเฉพาะคี่ p

ภาควิชา **คณิตศาสตร์** ลายมือชื่อนิสิต……………..…………….……………..

สาขาวิชา **คณิตศาสตร์** ลายมือชื่ออาจารย์ที่ปรึกษา……………………….…..

ปีการศึกษา 2544

427 24063 23 : MAJOR MATHEMATICS

KEY WORDS: GROUP ACTION / n-ELEMENT SUBSETS.

SIRINYA PRONGJIT : n-ELEMENT SUBSETS OF $\{1,2,\ldots,2n\}$ WHOSE SUMS ARE DIVISIBLE BY n. THESIS ADVISOR : ASST. PROF. PATTANEE UDOMKAVANICH, Ph.D., 33 pp. ISBN 974-17-0127-6.

In this research, we focus on the Problem 6 of the International Mathematical Olympaid examinations in 1995. The problem was as follows:

" Let p be an odd prime number. Find the number of subsets A of the set $\{1,2,\ldots,2p\}$ such that

(1) A has exactly p elements, and

(2) the sum of all elements in A is divisible by p."

This problem has at least 3 arguments in solving it. We present the fourth argument using a group action. Furthermore, we generalize this problem where p is replaced by any positive integer n.

Department **Mathematics** Student's signature....................................

Field of study **Mathematics** Advisor's signature....................................

Academic year **2001**

กิตติกรรมประกาศ

ผู้เขียนขอกราบขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร. พัฒนี อุดมกะวานิช อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ได้ดูแลเอาใจใส่ในทุกๆ เรื่องเป็นอย่างดีมาโดยตลอด โดยเฉพาะในส่วนของการเรียบเรียงวิทยานิพนธ์ ท่านได้อดทนยิ่งในการช่วยแก้ไขข้อบกพร่องต่างๆ ทำให้เกิดความสมบูรณ์แบบของวิทยานิพนธ์ฉบับนี้ ขอขอบคุณ อาจารย์ ดร. ศจี เพียรสกุล ที่ให้ความช่วยเหลือในส่วนของการใช้โปรแกรม Latex พิมพ์ภาษาไทย ทำให้การพิมพ์วิทยานิพนธ์ฉบับนี้เป็นไปด้วยความราบรื่น

ท้ายที่สุดนี้ขอกราบขอบพระคุณ คุณพ่อ คุณแม่ของผู้เขียน ที่ให้การส่งเสริมและสนับสนุนในเรื่องการศึกษา ตลอดจนเป็นกำลังใจ คอยรับฟัง และหาทางออกให้กับทุกปัญหาที่เกิดขึ้นตลอดระยะเวลาการศึกษา จนกระทั่งผู้เขียนมีวันนี้

สารบัญ

หน้า

บทนำ

ในการแข่งขันคณิตศาสตร์โอลิมปิกระหว่างประเทศ (IMO) มีโจทย์ปัญหาที่หลากหลายและท้าทายให้ค้นหาคำตอบ การที่จะได้มาซึ่งคำตอบที่ถูกต้องนั้นจะต้องใช้การวิเคราะห์ที่ลึกซึ้งและกระบวนการพิสูจน์ที่รัดกุม

ในวิทยานิพนธ์นี้ เราเล็งไปที่โจทย์ปัญหาข้อ 6 จากการแข่งขัน IMO (1995) ซึ่งเป็นโจทย์ปัญหาที่ได้รับความเห็นพ้องกันว่ายากที่สุดในบรรดาโจทย์ปัญหาทั้ง 6 ข้อจากการแข่งขันครั้งนั้น โจทย์ปัญหากล่าวว่า

" ให้ p เป็นจำนวนเฉพาะคี่ใดๆ จงหาจำนวนของสับเซต A ของเซต $\{1, 2, \ldots, 2p\}$ โดยที่ A มีสมบัติดังนี้

(i) A มีสมาชิก p ตัว และ

(ii) ผลบวกของสมาชิกใน A หารด้วย p ลงตัว "

โจทย์ปัญหาข้อนี้ไม่เพียงแต่ยากเท่านั้น หากยังมีความน่าสนใจในอีกแง่มุมคือ มีวิธีแก้ปัญหาโจทย์ข้อนี้หลากหลายวิธี วิธีแรก ผู้เสนอโจทย์ปัญหานี้ได้ให้ผลเฉลย โดยใช้เพียงความรู้พื้นฐานทางทฤษฎีจำนวนและหลักการนับ วิธีที่ 2 เป็นการแก้ปัญหาโดยใช้เทคนิคของฟังก์ชันก่อกำเนิดและความรู้เรื่องรากปฐมฐานที่ p ของ 1 วิธีที่ 3 ค้นพบโดยผู้นำทีมจากประเทศอิตาลี เป็นการแก้ปัญหาโดยผสมผสานความรู้ทางพีชคณิตนามธรรม ทฤษฎีจำนวน และคอมบินาทอริค เราจะเสนอการนำความรู้เรื่องการกระทำของกรุปบนเซตมาประยุกต์แก้ปัญหาเป็นวิธีที่ 4 และขยายขอบเขตของปัญหาเพื่อศึกษาผลเฉลยในกรณีจำนวนเต็มบวก n ใดๆ แทนที่จะเป็นจำนวนเฉพาะคี่ p

เนื้อหาในวิทยานิพนธ์นี้แบ่งออกเป็น 3 บท

บทที่ 1 เป็นการแนะนำบทนิยามและทฤษฎีบททั่วไปทางทฤษฎีจำนวน พีชคณิตนามธรรม และฟังก์ชันก่อกำเนิด เพื่อเป็นพื้นฐานในการศึกษาวิทยานิพนธ์นี้ อีกทั้งรวบรวมสมบัติต่างๆ ของรากปฐมฐานในสนามจำนวนเชิงซ้อนที่มีบทบาทในงานวิจัยนี้เพื่อใช้อ้างในบทถัดไป ตลอดจนกำหนดข้อตกลงเกี่ยวกับสัญลักษณ์ที่ใช้ในวิทยานิพนธ์ฉบับนี้

บทที่ 2 เป็นการเสนอวิธีต่างๆ ที่ใช้แก้ปัญหาข้างต้นซึ่งมี 4 วิธี

บทที่ 3 จะแสดงการหาผลเฉลยของปัญหาที่ขยายขอบเขตการศึกษาจากกรณีจำนวนเฉพาะคี่ p ไปสู่กรณีจำนวนเต็มบวก n ใดๆ

บทที่ 1

ความรู้พื้นฐาน

เราจะแบ่งเนื้อหาในบทนี้ออกเป็น 4 หัวข้อ หัวข้อ 1.1 เป็นการทบทวนบทนิยามและทฤษฎีบทของสมภาคและระบบส่วนตกค้างบริบูรณ์เท่าที่จำเป็นสำหรับการศึกษาวิทยานิพนธ์ฉบับนี้ หัวข้อ 1.2 จะเสนอบทนิยามของรากปฐมฐานในสนามจำนวนเชิงซ้อนและสมบัติสำคัญต่างๆ ซึ่งเราได้รวบรวมเพื่อใช้อ้างในบทที่ 2 และบทที่ 3 อีกทั้งทบทวนบทนิยามของพหุนามเล็กสุดเฉพาะกลุ่มและทฤษฎีบทซึ่งต้องใช้ในวิทยานิพนธ์นี้ หัวข้อ 1.3 เป็นการทบทวนความรู้เรื่องการกระทำของกรุปบนเซตเฉพาะที่ใช้ในวิทยานิพนธ์ และหัวข้อ 1.4 จะแนะนำบทนิยามของฟังก์ชันก่อกำเนิดและตัวอย่างการนำไปใช้ประโยชน์เพื่อเป็นพื้นฐานในการศึกษาวิทยานิพนธ์ต่อไป

ก่อนอื่นจะกำหนดข้อตกลงเกี่ยวกับสัญลักษณ์ที่ต้องใช้ในวิทยานิพนธ์ดังนี้

ข้อตกลงเกี่ยวกับสัญลักษณ์ที่ใช้ในวิทยานิพนธ์

$\mathbb{N}$	หมายถึง	เซตของจำนวนเต็มบวกทั้งหมด
$\mathbb{N}_0$	หมายถึง	$\mathbb{N} \cup \{0\}$
$\mathbb{E}$	หมายถึง	เซตของจำนวนเต็มบวกคู่ทั้งหมด
$\mathbb{O}$	หมายถึง	เซตของจำนวนเต็มบวกคี่ทั้งหมด
$\mathbb{Q}$	หมายถึง	เซตของจำนวนตรรกยะทั้งหมด
S_{2n}	หมายถึง	$\{1, 2, \ldots, 2n\}$ ทุก $n \in \mathbb{N}$
$\lvert A\rvert$	หมายถึง	จำนวนของสมาชิกในเซต A
$m \mid n$	หมายถึง	m หาร n ลงตัว
(m, n)	หมายถึง	ห.ร.ม. ของ m และ n
$\phi(n)$	หมายถึง	จำนวนของจำนวนเต็มบวกทั้งหมดที่ไม่เกิน n และเป็นจำนวนเฉพาะสัมพัทธ์กับ n

1.1. สมภาคและระบบส่วนตกค้างบริบูรณ์

บทนิยาม 1.1.1. ให้ n เป็นจำนวนเต็มบวกใดๆ จำนวนเต็ม k และ l **สมภาคกัน (congruent)** มอดุโล n หรือกล่าวว่า k **สมภาคกับ** l **มอดุโล** n ซึ่งเขียนแทนด้วยสัญลักษณ์ $k \equiv l \pmod{n}$ ก็ต่อเมื่อ $n \mid (k - l)$

ถ้า k ไม่สมภาคกับ l มอดุโล n จะเขียนแทนด้วยสัญลักษณ์ $k \not\equiv l \pmod{n}$

ทฤษฎีบท 1.1.2. สำหรับจำนวนเต็ม k, l, m และ n ใดๆ โดยที่ n เป็นจำนวนเต็มบวก จะได้ว่า

(i) $k \equiv l \pmod{n}$ ก็ต่อเมื่อ $m + k \equiv m + l \pmod{n}$

(ii) ถ้า $mk \equiv ml \pmod{n}$ และ $(m,n) = 1$ แล้ว $k \equiv l \pmod{n}$

บทนิยาม 1.1.3. เซตของจำนวนเต็ม $\{k_1, k_2, \ldots, k_n\}$ เป็น **ระบบส่วนตกค้างบริบูรณ์ (complete residue system)** มอดุโล n ก็ต่อเมื่อ ทุกๆ จำนวนเต็ม k จะมีจำนวนเต็ม k_i เพียงตัวเดียวที่ทำให้ $k \equiv k_i \pmod{n}$

ข้อสังเกต

(i) เซต $\{0, 1, \ldots, n-1\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n

(ii) เซต $\{k_1, k_2, \ldots, k_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n ก็ต่อเมื่อ ทุกๆ $i \neq j$ $k_i \not\equiv k_j (\mathrm{mod}\ n)$

ทฤษฎีบท 1.1.4. ให้ m และ n เป็นจำนวนเต็มบวกซึ่ง $(m,n) = 1$ ถ้า $\{k_1, k_2, \ldots, k_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n แล้ว สำหรับทุกจำนวนเต็ม i

$$\{i + k_1 m, i + k_2 m, \ldots, i + k_n m\} \text{ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล } n$$

บทพิสูจน์. ให้ $j, j^{'} \in \{1, 2, \ldots, n\}$ โดยที่ $j \neq j^{'}$ จะได้ว่า $k_j \not\equiv k_{j'} \pmod{n}$
เนื่องจาก $(m,n) = 1$ ดังนั้นเราได้โดยทฤษฎีบท 1.1.2(ii) ว่า $k_j m \not\equiv k_{j'} m (\mathrm{mod}\ n)$
โดยทฤษฎีบท 1.1.2(i) สรุปได้ว่า $i + k_j m \not\equiv i + k_{j'} m (\mathrm{mod}\ n)$ ทุกจำนวนเต็ม i
ฉะนั้น สำหรับแต่ละจำนวนเต็ม i

$$\{i + k_1 m, i + k_2 m, \ldots, i + k_n m\} \text{ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล } n$$

□

1.2. รากปฐมฐานที่ n ของ 1 ในสนามจำนวนเชิงซ้อนและพหุนามเล็กสุดเฉพาะกลุ่ม

บทนิยาม 1.2.1. ให้ n เป็นจำนวนเต็มบวกใดๆ เราจะเรียกรากเชิงซ้อนของพหุนาม $x^n - 1$ ว่า **รากที่ n ของ 1 (nth root of unity)** และจะเรียกรากที่ n ของ 1 ว่า **รากปฐมฐานที่ n ของ 1 (primitive nth root of unity)** ถ้ารากดังกล่าวไม่เป็นรากที่ d ของ 1 ทุกจำนวนเต็มบวก $d < n$

ทฤษฎีบท 1.2.2. ([1]) ให้ n เป็นจำนวนเต็มบวกใดๆ จะได้ว่า $\zeta_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$ เป็นรากปฐมฐานที่ n ของ 1

ทฤษฎีบท 1.2.3. ([5]) ให้ n เป็นจำนวนเต็มบวกใดๆ และ ζ เป็นรากปฐมฐานที่ n ของ 1 จะได้ว่า

(i) สำหรับจำนวนเต็มบวก m ใดๆ $\zeta^m = 1$ ก็ต่อเมื่อ $n | m$

(ii) $\{1 = \zeta^0, \zeta, \ldots, \zeta^{n-1}\}$ เป็นเซตของรากที่ n ซึ่งแตกต่างกันทั้งหมดของ 1

ทฤษฎีบท 1.2.4. ([3]) ให้ F เป็นสนามใดๆ จะได้ว่า

(i) ถ้าพหุนาม $f(x) \in F[x] \setminus F$ มีดีกรีเท่ากับ n แล้ว $f(x)$ จะมีรากในสนาม $K \supseteq F$ ใดๆ ได้ไม่เกิน n ราก

(ii) ถ้า $a_1, a_2, \ldots, a_n$ เป็นรากทั้งหมดของ $f(x)$ แล้ว

$$f(x) = k \prod_{i=1}^{n} (x - a_i) \qquad \text{โดยที่ } k \in F$$

บทแทรก 1.2.5. ให้ n เป็นจำนวนเต็มบวกใดๆ และ ζ เป็นรากปฐมฐานที่ n ของ 1 จะได้ว่า

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta^i)$$

ยิ่งกว่านั้น

$$a^n - 1 = \prod_{i=0}^{n-1} (a - \zeta^i) \quad \text{ทุกจำนวนเชิงซ้อน } a$$

ทฤษฎีบท 1.2.6. ให้ n เป็นจำนวนเต็มบวกใดๆ และ ζ เป็นรากปฐมฐานที่ n ของ 1 จะได้ว่า

(i) สำหรับจำนวนเต็มบวก m ใดๆ ζ^m เป็นรากปฐมฐานที่ n ของ 1 ก็ต่อเมื่อ $(m,n) = 1$

(ii) สำหรับแต่ละจำนวนเต็ม $i \geq 0$ และจำนวนเต็มบวก m ซึ่ง $(m,n) = 1$ ถ้า $\{k_1, k_2, \ldots, k_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n แล้ว

$$\{\zeta^{i+k_1 m}, \zeta^{i+k_2 m}, \ldots, \zeta^{i+k_n m}\}$$

เป็นเซตของรากที่ n ซึ่งแตกต่างกันทั้งหมดของ 1

บทพิสูจน์. (i) ($\Rightarrow$) สมมติ ζ^m เป็นรากปฐมฐานที่ n ของ 1 โดยทฤษฎีบท 1.2.3 (ii) จะได้ว่า

$$\zeta = \zeta^{mk} \quad \text{สำหรับจำนวนเต็ม } k \text{ บางตัวซึ่ง } 0 \leq k \leq n-1$$

ฉะนั้น $1 = \zeta^{mk-1}$ โดยทฤษฎีบท 1.2.3 (i) เราได้ว่า $n | mk - 1$ ดังนั้น

$$mk - 1 = nl \quad \text{สำหรับจำนวนเต็ม } l \text{ บางตัว}$$

จึงได้ว่า $mk - nl = 1$ นั่นคือ $(m,n) = 1$

($\Leftarrow$) สมมติ $(m,n) = 1$ ถ้า ζ^m ไม่เป็นรากปฐมฐานที่ n ของ 1 แล้ว

$$\zeta^{md} = 1 \quad \text{สำหรับจำนวนเต็มบวก } d \text{ บางตัวซึ่ง } d < n$$

พิจารณา

$$md = qn + r \quad \text{เมื่อ } q \text{ และ } r \text{ เป็นจำนวนเต็มซึ่ง } 0 \leq r < n$$

จะได้

$$1 = \zeta^{md} = \zeta^{qn+r} = \zeta^r$$

ดังนั้น $r = 0$ จึงได้ว่า $n | md$ แต่ $(m,n) = 1$ ดังนั้น $n | d$ ซึ่งเป็นไปไม่ได้เพราะ $1 \leq d < n$

(ii) ให้ i เป็นจำนวนเต็มซึ่ง $i \geq 0$
เนื่องจาก $(m,n)=1$ และ $\{k_1,k_2,\ldots,k_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n ดังนั้นเราได้โดยทฤษฎีบท 1.1.4 ว่า

$$\{i+k_1m, i+k_2m, \ldots, i+k_nm\} \quad \text{เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล } n$$

สมมติ $\zeta^{i+k_jm} = \zeta^{i+k_{j'}m}$ โดยที่ $j,j' \in \{1,2,\ldots,n\}$
จะได้ว่า $\zeta^{(i+k_jm)-(i+k_{j'}m)} = 1$
ดังนั้น $n|(i+k_jm)-(i+k_{j'}m)$ นั่นคือ $i+k_jm \equiv i+k_{j'}m \pmod n$
จึงสรุปได้ว่า

$$\{\zeta^{i+k_1m}, \zeta^{i+k_2m}, \ldots, \zeta^{i+k_nm}\} \text{ เป็นเซตของรากที่ } n \text{ ซึ่งแตกต่างกันทั้งหมดของ } 1$$

□

ทฤษฎีบท 1.2.7. ให้ n เป็นจำนวนเต็มบวกคี่ใดๆ และ ζ เป็นรากปฐมฐานที่ n ของ 1 จะได้ว่า

$$x^n + 1 = \prod_{k=0}^{n-1}\left(x+\zeta^k\right)$$

บทพิสูจน์. เนื่องจาก n เป็นจำนวนเต็มบวกคี่ ดังนั้น

$$\begin{aligned} x^n + 1 &= (-1)\left((-x)^n - 1\right) \\ &= (-1)\prod_{k=0}^{n-1}\left(-x-\zeta^k\right) \\ &= (-1)(-1)^n\prod_{k=0}^{n-1}\left(x+\zeta^k\right) \\ &= \prod_{k=0}^{n-1}\left(x+\zeta^k\right) \end{aligned}$$

□

ทฤษฎีบท 1.2.8. ให้ n เป็นจำนวนเต็มบวกใดๆ และ ζ เป็นรากปฐมฐานที่ n ของ 1 จะได้ว่า

(i) ถ้า n เป็นจำนวนคู่แล้ว $\zeta^{\frac{n}{2}} = -1$

(ii) สำหรับจำนวนเต็มบวก d ซึ่ง $d|n$ จะได้ว่า ζ^d เป็นรากปฐมฐานที่ $\frac{n}{d}$ ของ 1

(iii) สำหรับจำนวนเต็มบวก m ซึ่ง $(m,n)=d$ จะได้ว่า ζ^m เป็นรากปฐมฐานที่ $\frac{n}{d}$ ของ 1

บทนิยาม 1.2.9. ให้ K และ F เป็นสนามซึ่ง $K \supseteq F$ เราจะเรียกพหุนาม $f \in F[x]\backslash\{0\}$ ว่า **พหุนามเล็กสุดเฉพาะกลุ่ม (the minimal polynomial) ของ** $a(\in K)$ **บน** F ถ้า f เป็นพหุนามลดทอนไม่ได้ (irreducible polynomial) ใน $F[x]$ ซึ่งมี a เป็นราก และสัมประสิทธิ์ของพจน์กำลังสูงสุดเป็น 1

ทฤษฎีบท 1.2.10. ([5]) ให้ p เป็นจำนวนเฉพาะคี่ใดๆ และ ζ เป็นรากปฐมฐานที่ p ของ 1 จะได้ว่า $1+x+\ldots+x^{p-1}$ เป็นพหุนามเล็กสุดเฉพาะกลุ่มของ ζ บน $\mathbb{Q}$

1.3. การกระทำของกรุปบนเซต

บทนิยาม 1.3.1. การกระทำ (action) ของกรุป G บนเซต S คือฟังก์ชัน $G\times S\to S$ ซึ่งมีสมบัติว่า ทุก $x\in S$

(i) $ex=x$ เมื่อ e คือเอกลักษณ์ของกรุป G

(ii) $(g_1g_2)x=g_1(g_2x)$ ทุก $g_1,g_2\in G$

เมื่อการกระทำถูกกำหนดไว้แล้วเราจะกล่าวว่า G **กระทำบนเซต** S หรือ S เป็น $G-$เซต ($G-\mathrm{set}$)

บทนิยาม 1.3.2. ให้กรุป G กระทำบนเซต S **วงโคจร (orbit)**ของ $x\in S$ คือเซต

$$\{gx\mid g\in G\}$$

เราจะเขียนแทนวงโคจรของ $x\in S$ ด้วยสัญลักษณ์ $orb(x)$

ทฤษฎีบท 1.3.3. ([2]) ให้กรุป G กระทำบนเซต S จะได้ว่า เซตของวงโคจรของ x ทั้งหมดใน S ($\{orb(x)\mid x\in S\}$) เป็นผลแบ่งกั้นของเซต S

1.4. ฟังก์ชันก่อกำเนิด

บทนิยาม 1.4.1. ให้ $(a_{r,s})=(a_{0,0},a_{0,1},\ldots,a_{0,k_0},a_{1,0},a_{1,1},\ldots,a_{1,k_1},\ldots,a_{n,0},a_{n,1},\ldots,a_{n,k_n})$ เราจะเรียก $(a_{r,s})$ ว่า **แถวลำดับสองชั้น (double array)**

บทนิยาม 1.4.2. ให้ $(a_{r,s})=(a_{0,0},a_{0,1},\ldots,a_{0,k_0},a_{1,0},a_{1,1},\ldots,a_{1,k_1},\ldots,a_{n,0},a_{n,1},\ldots,a_{n,k_n})$ เป็นแถวลำดับสองชั้น เราจะเรียก $g(x,y)$ ว่า **ฟังก์ชันก่อกำเนิด (generating function)** ของ $(a_{r,s})$ ก็ต่อเมื่อ

$$g(x,y)=\sum_{r=0}^{n}\sum_{s=0}^{k_r}a_{r,s}x^ry^s$$

เราสามารถใช้ฟังก์ชันก่อกำเนิดนับจำนวนของสิ่งที่ต้องการซึ่งมีเงื่อนไข 2 อย่างได้ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 1.4.3. ให้ $a_{r,s}$ เป็นจำนวนวิธีที่เราสามารถเขียน s ให้อยู่ในรูปของผลบวกของจำนวนเต็มบวก r จำนวนซึ่งแตกต่างกันทั้งหมดในเซต $\{1,2,\ldots,n\}$
เราจะสร้างฟังก์ชันก่อกำเนิด $g(x,y)$ ซึ่งสัมประสิทธิ์ของ x^ry^s เท่ากับ $a_{r,s}$ ดังนี้

พิจารณาระบบสมการต่อไปนี้

$$\begin{aligned} e_1 + e_2 + \ldots + e_n &= r \qquad (1)\\ 1e_1 + 2e_2 + \ldots + ne_n &= s \qquad (2) \end{aligned}$$

เมื่อ $e_i \in \{0,1\}$ ทุก $i \in \{1,2,\ldots,n\}$

จะเห็นว่า $a_{r,s}$ คือจำนวนของผลเฉลยของระบบสมการข้างต้น ซึ่งส่งผลให้เราได้อีกหนึ่งมุมมองว่า $a_{r,s}$ คือจำนวนวิธีเขียน x^ry^s ให้อยู่ในรูปของผลคูณของพจน์จำนวน n พจน์โดยมีรูปแบบดังนี้

$$\begin{Bmatrix} (x^1y^1)^0 \\ (x^1y^1)^1 \end{Bmatrix} \begin{Bmatrix} (x^1y^2)^0 \\ (x^1y^2)^1 \end{Bmatrix} \ldots \begin{Bmatrix} (x^1y^n)^0 \\ (x^1y^n)^1 \end{Bmatrix}$$

โดยที่ พจน์ที่ 1 เลือกตัวใดตัวหนึ่งจาก $\begin{Bmatrix} (x^1y^1)^0 \\ (x^1y^1)^1 \end{Bmatrix}$

พจน์ที่ 2 เลือกตัวใดตัวหนึ่งจาก $\begin{Bmatrix} (x^1y^2)^0 \\ (x^1y^2)^1 \end{Bmatrix}$

$\vdots$

พจน์ที่ n เลือกตัวใดตัวหนึ่งจาก $\begin{Bmatrix} (x^1y^n)^0 \\ (x^1y^n)^1 \end{Bmatrix}$

หรืออีกนัยหนึ่ง $a_{r,s}$ คือจำนวนวิธีเลือกแต่ละพจน์ของพหุนาม

$\left((x^1y^1)^0 + (x^1y^1)^1\right), \left((x^1y^2)^0 + (x^1y^2)^1\right), \ldots, \left((x^1y^n)^0 + (x^1y^n)^1\right)$ ซึ่งนำมาคูณกันแล้วได้ x^ry^s

ฉะนั้น $a_{r,s}$ คือสัมประสิทธิ์ของ x^ry^s ของพหุนาม

$$\left((x^1y^1)^0 + (x^1y^1)^1\right)\left((x^1y^2)^0 + (x^1y^2)^1\right)\ldots\left((x^1y^n)^0 + (x^1y^n)^1\right)$$

เนื่องจาก

$$\left((x^1y^1)^0 + (x^1y^1)^1\right)\left((x^1y^2)^0 + (x^1y^2)^1\right)\ldots\left((x^1y^n)^0 + (x^1y^n)^1\right) = (1+xy)\left(1+xy^2\right)\ldots(1+xy^n)$$

ฉะนั้น $g(x,y) = \prod_{i=1}^{n}\left(1+xy^i\right)$ คือฟังก์ชันก่อกำเนิดของแถวลำดับสองชั้น $(a_{r,s})$

เราจะทราบค่าของ $a_{r,s}$ ได้โดยการคำนวนสัมประสิทธิ์ของ x^ry^s ของพหุนาม $\prod_{i=1}^{n}\left(1+xy^i\right)$

เช่นกรณี $n=6$ เราหาค่าของ $a_{3,8}$ ได้จากการพิจารณาพหุนาม

$$g(x,y) = (1+xy)(1+xy^2)(1+xy^3)(1+xy^4)(1+xy^5)(1+xy^6)$$

เนื่องจาก

$$\begin{aligned} x^3y^8 = xyxy^2xy^5 &\quad\Leftrightarrow\quad 8 = 1+2+5\\ x^3y^8 = xyxy^3xy^4 &\quad\Leftrightarrow\quad 8 = 1+3+4 \end{aligned}$$

ฉะนั้น เราสามารถเขียน 8 ให้อยู่ในรูปของผลบวกของจำนวนเต็มบวก 3 จำนวนซึ่งแตกต่างกันทั้งหมด ในเซต $\{1, 2, 3, 4, 5, 6\}$ ได้ 2 วิธี

บทที่ 2

ผลเฉลยกรณี p เป็นจำนวนเฉพาะคี่โดยวิธีต่างๆ

ในบทนี้ เราจะเสนอวิธีต่างๆ ที่ใช้แก้โจทย์ปัญหาดังได้เกริ่นไว้ในบทนำ และเพื่อเป็นการทบทวนเราขอเสนอโจทย์ปัญหาในรูปแบบทฤษฎีบทดังนี้

ทฤษฎีบท 2.1. ให้ p เป็นจำนวนเฉพาะคี่ใดๆ จะได้ว่า จำนวนของสับเซต A ทั้งหมดของเซต S_{2p} ซึ่งมีสมบัติว่า

(i) A มีสมาชิก p ตัว และ

(ii) ผลบวกของสมาชิกในเซต A หารด้วย p ลงตัว

คือ

$$\frac{1}{p}\left(\binom{2p}{p}-2\right)+2$$

หรืออีกนัยหนึ่ง ถ้าเราให้ $\mathcal{D}_p=\left\{A\subseteq S_{2p}\mid |A|=p \text{ และ } p\mid \sum_{x\in A}x\right\}$ แล้ว

$$|\mathcal{D}_p|=\frac{1}{p}\left(\binom{2p}{p}-2\right)+2$$

เราจะแบ่งวิธีพิสูจน์ทฤษฎีบท 2.1 ในแบบต่างๆ เป็น 4 หัวข้อ หัวข้อ 2.1 จะแสดงการพิสูจน์โดยใช้เพียงความรู้พื้นฐานทางทฤษฎีจำนวนและหลักการนับ ซึ่งเป็นวิธีที่ผู้เสนอโจทย์ปัญหานี้ได้เฉลย หัวข้อ 2.2 เรานำความรู้เรื่องการกระทำของกรุปบนเซตมาใช้แก้ปัญหา โดยพิจารณาเซตของสับเซตที่มีสมาชิก p ตัวทั้งหมดของเซต S_{2p} เป็น $\mathbb{Z}_p-$เซต เมื่อ $\mathbb{Z}_p$ เป็นกรุปภายใต้การบวกของจำนวนเต็มมอดุโล p หัวข้อ 2.3 เสนอการพิสูจน์โดยใช้เทคนิคของฟังก์ชันก่อกำเนิดและความรู้เรื่องรากปฐมฐานที่ p ของ 1 ส่วนหัวข้อ 2.4 เป็นการพิสูจน์โดยผสมผสานความรู้ทางพีชคณิตนามธรรม ทฤษฎีจำนวน และคอมบินาทอริค

สัญลักษณ์เพิ่มเติมที่ใช้เฉพาะหัวข้อ 2.1 และ 2.2

สำหรับแต่ละ p เป็นจำนวนเฉพาะคี่ใดๆ

U_p	หมายถึง	เซตของสับเซตที่มีสมาชิก p ตัวทั้งหมดของเซต S_{2p}
L	หมายถึง	$\{1, 2, \ldots, p\}$
R	หมายถึง	$\{p+1, p+2, \ldots, 2p\}$
A_L	หมายถึง	$A \cap L$
A_R	หมายถึง	$A \cap R$
$\sigma(A)$	หมายถึง	ผลบวกมอดุโล p ของสมาชิกในเซต A
$x \oplus A$	หมายถึง	$\{x + a \pmod{p} \mid a \in A\}$

2.1. ผลเฉลยกรณี p เป็นจำนวนเฉพาะคี่โดยการใช้ความรู้พื้นฐานทางทฤษฎีจำนวน . และหลักการนับ

ก่อนจะแสดงการพิสูจน์ทฤษฎีบท 2.1 โดยวิธีนี้ เราจะเสนอการวิเคราะห์กรณีตัวอย่าง $p = 3$ และ $p = 5$ เพื่อให้เห็นแนวคิดดังนี้

วิเคราะห์กรณีตัวอย่าง $p = 3$ และ $p = 5$

กรณี $p = 3$ พิจารณาเซต $S_6 = \{1, 2, 3, 4, 5, 6\}$ เราสังเกตเห็นว่า

ผลบวกของสมาชิกในเซต $\{1, 2, 3\}$ เท่ากับ $6 \equiv 0 \pmod{3}$ และ
ผลบวกของสมาชิกในเซต $\{4, 5, 6\}$ เท่ากับ $15 \equiv 0 \pmod{3}$

ดังนั้น $\{1, 2, 3\}$ และ $\{4, 5, 6\}$ เป็นสมาชิกของ $\mathcal{D}_3$

เมื่อพิจารณาสับเซตที่เหลือของ S_6 ที่มีสมาชิก 3 ตัว ซึ่งมีทั้งสิ้น $\binom{6}{3} - 2$ สับเซต เราสามารถแบ่งสับเซตเหล่านี้ออกเป็น 3 กลุ่ม โดยที่
กลุ่มที่ 1 ประกอบด้วยสับเซตที่มีสมบัติว่า ผลบวกของสมาชิกในสับเซตสมภาคกับ 0 มอดุโล 3
กลุ่มที่ 2 ประกอบด้วยสับเซตที่มีสมบัติว่า ผลบวกของสมาชิกในสับเซตสมภาคกับ 1 มอดุโล 3 และ
กลุ่มที่ 3 ประกอบด้วยสับเซตที่มีสมบัติว่า ผลบวกของสมาชิกในสับเซตสมภาคกับ 2 มอดุโล 3
ได้กลุ่มละเท่าๆ กันดังนี้

กลุ่มที่ 1	กลุ่มที่ 2	กลุ่มที่ 3
$\{2,3,4\}$	$\{1,2,4\}$	$\{1,3,4\}$
$\{1,3,5\}$	$\{2,3,5\}$	$\{1,2,5\}$
$\{1,2,6\}$	$\{1,3,6\}$	$\{2,3,6\}$
$\{3,4,5\}$	$\{1,4,5\}$	$\{2,4,5\}$
$\{2,4,6\}$	$\{3,4,6\}$	$\{1,4,6\}$
$\{1,5,6\}$	$\{2,5,6\}$	$\{3,5,6\}$

แผนภาพที่ 1

ดังนั้น จำนวนของสับเซตทั้งหมดใน $\mathcal{D}_3$ คือ $6+2=8$ สับเซต ซึ่ง 6 ได้มาจาก $\frac{1}{3}\left(\binom{6}{3}-2\right)$ (คือจำนวนของสับเซตในแต่ละกลุ่มจากการแบ่งสับเซตจำนวน $\binom{6}{3}-2$ เซตออกเป็น 3 กลุ่มๆ ละเท่าๆ กัน) และ 2 ได้มาจากการนับเซต $\{1,2,3\}$ และเซต $\{4,5,6\}$ จึงคาดเดาว่าคำตอบของปัญหานี้คือ

$$\frac{1}{p}\left(\binom{2p}{p}-2\right)+2$$

กรณี $p=5$ พิจารณาเซต $S_{10}=\{1,2,3,4,5,6,7,8,9,10\}$ สังเกตเห็นได้โดยง่ายว่า

$\{1,2,3,4,5\}$ และ $\{6,7,8,9,10\}$ เป็นสมาชิกของ $\mathcal{D}_5$

เมื่อพิจารณาสับเซตที่เหลือของ S_{10} ที่มีสมาชิก 5 ตัวซึ่งมีทั้งสิ้น $\binom{10}{5}-2=250$ สับเซต เป็นความไม่สะดวกที่จะแบ่งสับเซตเหล่านี้ออกเป็น 5 กลุ่ม โดยให้ผลบวกของสมาชิกในสับเซตที่อยู่ในกลุ่มเดียวกัน**สมภาคกัน**มอดุโล 5 เพราะสมาชิกในแต่ละกลุ่มมีเป็นจำนวนมาก ทำให้เราหาความสัมพันธ์ของสมาชิกในกลุ่มได้ยาก ฉะนั้นแทนที่จะแบ่งสับเซตเหล่านี้ออกเป็น 5 กลุ่มตามลักษณะดังกล่าว เราน่าจะแบ่งสับเซตเหล่านี้ออกเป็นกลุ่มละ 5 สับเซต โดยให้เซตของผลบวกของสมาชิกในแต่ละสับเซตของแต่ละกลุ่มเป็น**ระบบส่วนตกค้างบริบูรณ์**มอดุโล 5 หากเราทำได้จำนวนของสับเซตทั้งหมดใน $\mathcal{D}_5$ ก็คือจำนวนของกลุ่มทั้งหมดบวกด้วยสอง

เมื่อย้อนกลับไปมองกรณี $p=3$ จากแผนภาพที่ 1 เราปรับมุมมองใหม่ดังนี้

กลุ่มที่ 1	$\{2,3,4\}$	$\{1,2,4\}$	$\{1,3,4\}$
กลุ่มที่ 2	$\{1,3,5\}$	$\{2,3,5\}$	$\{1,2,5\}$
กลุ่มที่ 3	$\{1,2,6\}$	$\{1,3,6\}$	$\{2,3,6\}$
กลุ่มที่ 4	$\{3,4,5\}$	$\{1,4,5\}$	$\{2,4,5\}$
กลุ่มที่ 5	$\{2,4,6\}$	$\{3,4,6\}$	$\{1,4,6\}$
กลุ่มที่ 6	$\{1,5,6\}$	$\{2,5,6\}$	$\{3,5,6\}$

แผนภาพที่ 2

แผนภาพที่ 2 แสดงการแบ่งกลุ่มสับเซตที่มีสมาชิก 3 ตัวของเซต S_6 ที่เหลือจากการแยกเซต $\{1,2,3\}$ และ $\{4,5,6\}$ ไว้ต่างหาก ซึ่งแต่ละกลุ่มประกอบด้วย 3 สับเซต และเซตของผลบวกของสมาชิกในแต่ละสับเซตของแต่ละกลุ่มเป็นระบบส่วนตกค้างบริบูรณ์มอดุโล 3

การแบ่งกลุ่มตามที่ปรากฏในแผนภาพที่ 2 ให้ข้อสังเกตว่า สับเซต A และ B ที่อยู่ในกลุ่มเดียวกันมีความเกี่ยวข้องกันดังนี้

(i) $B \cap \{1,2,3\} = x \oplus (A \cap \{1,2,3\})$ สำหรับบาง $x \in \{0,1,2\}$

(ii) $B \cap \{4,5,6\} = A \cap \{4,5,6\}$

แนวคิด จากการวิเคราะห์กรณีตัวอย่าง $p = 3$ และ $p = 5$ เราน่าจะพิสูจน์ทฤษฎีบท 2.1 โดยแยกเซต S_{2p} เป็น $L = \{1,2,\ldots,p\}$ และ $R = \{p+1, p+2, \ldots, 2p\}$ ซึ่งเราทราบว่า

ผลบวกของสมาชิกในเซต L เท่ากับ $\frac{p(p+1)}{2} \equiv 0 \pmod p$ และ
ผลบวกของสมาชิกในเซต R เท่ากับ $\frac{p(3p+1)}{2} \equiv 0 \pmod p$

นั่นคือ L และ R เป็นสมาชิกของ $\mathcal{D}_p$

ต่อไปแบ่งสับเซตใน $U_p \backslash \{L,R\}$ ซึ่งมีจำนวน $\binom{2p}{p} - 2$ สับเซตออกเป็นกลุ่มละ p สับเซต โดยแต่ละกลุ่มประกอบด้วยสับเซตดังต่อไปนี้

$$\begin{array}{rcccl} A & = & A_L & \cup & A_R, \\ & & (1 \oplus A_L) & \cup & A_R, \\ & & (2 \oplus A_L) & \cup & A_R, \\ & & & \vdots & \\ & & (p-1 \oplus A_L) & \cup & A_R \end{array}$$

สังเกตเห็นว่า สำหรับแต่ละ $A \in U_p \backslash \{L,R\}$ จะได้ $A_L \neq \emptyset$ และ $A_R \neq \emptyset$

เราอาศัยสมบัติพิเศษของจำนวนเฉพาะตั้งสมมติฐานว่า

(i) $A_L \cup A_R, (1 \oplus A_L) \cup A_R, \ldots, (p-1 \oplus A_L) \cup A_R$ เป็นเซตที่แตกต่างกันทั้งหมด

(ii) $\{\sigma((x \oplus A_L) \cup A_R) \mid x \in \{0,1,\ldots,p-1\}\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล p

(iii) แต่ละสับเซต $A \in U_p \backslash \{L,R\}$ ต้องปรากฏในกลุ่มหนึ่งเพียงกลุ่มเดียวเท่านั้น

หากเราสามารถพิสูจน์ได้ว่าสมมติฐานดังกล่าวจริง การแบ่งสับเซตใน $U_p \backslash \{L,R\}$ ลักษณะดังกล่าวย่อมทำให้เกิดผลแบ่งกั้นของเซต $U_p \backslash \{L,R\}$ ซึ่งแต่ละเซตในผลแบ่งกั้นมีสมาชิก p ตัวและมีสมาชิกเพียงหนึ่งตัวที่อยู่ใน $\mathcal{D}_p$

บทพิสูจน์ของทฤษฎีบท 2.1. .

ให้ p เป็นจำนวนเฉพาะคี่ใดๆ

เนื่องจาก $\sigma(L) \equiv \sigma(R) \equiv 0 \pmod{p}$ ดังนั้น L และ R เป็นสมาชิกของ $\mathcal{D}_p$

ต่อไปจะแบ่งสับเซตใน $U_p \backslash \{L, R\}$ ออกเป็นกลุ่มละ p สับเซต โดยกลุ่มที่มี A ประกอบด้วยสับเซตดังต่อไปนี้

$$\begin{array}{ccc} A_L & \cup & A_R, \\ (1 \oplus A_L) & \cup & A_R, \\ (2 \oplus A_L) & \cup & A_R, \\ & \vdots & \\ (p-1 \oplus A_L) & \cup & A_R \end{array}$$

เราต้องการแสดงว่า

(i) $A_L \cup A_R, (1 \oplus A_L) \cup A_R, \ldots, (p-1 \oplus A_L) \cup A_R$ เป็นเซตที่แตกต่างกันทั้งหมด

(ii) $\{\sigma((x \oplus A_L) \cup A_R) \mid x \in \{0, 1, \ldots, p-1\}\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล p

(iii) แต่ละสับเซต $A \in U_p \backslash \{L, R\}$ ต้องปรากฏในกลุ่มเพียงกลุ่มเดียวเท่านั้น

พิสูจน์ (i) สมมติว่า $(x \oplus A_L) \cup A_R = (y \oplus A_L) \cup A_R$ โดยที่ $x, y \in \{0, 1, \ldots, p-1\}$

ดังนั้น $x \oplus A_L = y \oplus A_L$ จึงได้ว่า $\sigma(x \oplus A_L) = \sigma(y \oplus A_L)$

ให้ $A_L = \{a_1, \ldots, a_k\}$ มีสมาชิก k ตัว

จะได้ว่า $\sigma(\{x + a_1, \ldots, x + a_k\}) = \sigma(\{y + a_1, \ldots, y + a_k\})$

ฉะนั้น

$$\sum_{i=1}^{k} (x + a_i) \equiv \sum_{i=1}^{k} (y + a_i) \pmod{p}$$

จึงได้ว่า $kx \equiv ky \pmod{p}$ นั่นคือ $p \mid k(x - y)$

เนื่องจาก $(k, p) = 1$ และ $0 \leq |x - y| < p$ ดังนั้น $x = y$

จึงสรุปได้ว่า (i) จริง

พิสูจน์ (ii) เป็นผลโดยตรงจากการพิสูจน์ (i) เพราะว่า

$$\sigma((x \oplus A_L) \cup A_R) = \sigma((y \oplus A_L) \cup A_R) \Rightarrow \sigma(x \oplus A_L) = \sigma(y \oplus A_L)$$

ทุก $x, y \in \{0, 1, \ldots, p-1\}$

พิสูจน์ (iii) สมมติให้ C เป็นสับเซตที่อยู่ในกลุ่มที่มี A และอยู่ในกลุ่มที่มี B ดังนั้น

$$C = (x \oplus A_L) \cup A_R = (y \oplus B_L) \cup B_R$$

เนื่องจาก $A_R = C_R = B_R$ ดังนั้น $x \oplus A_L = y \oplus B_L$

เราตรวจสอบได้ไม่ยากว่า ทุกจำนวนเต็ม a และ b

$$x + a \equiv y + b \pmod{p} \Leftrightarrow (x - y) + a \equiv b \pmod{p}$$

โดยไม่เสียนัยทั่วไป สมมติว่า $x \geq y$ ฉะนั้น เราสรุปได้ว่า

$$(x-y) \oplus A_L = B_L \qquad \text{และ} \;\; x-y \in \{0,1,\ldots,p-1\}$$

นั่นคือเซต A และ B อยู่ในกลุ่มเดียวกัน จึงได้ว่า

$$\{(x \oplus A_L) \cup A_R \mid x = 0,1,\ldots,p-1\} = \{(y \oplus B_L) \cup B_R \mid y = 0,1,\ldots,p-1\}$$

สรุปได้ว่า (iii) จริง

จากสมบัติข้อ (iii) เราได้ว่า การแบ่งกลุ่มสับเซตใน $U_p \backslash \{L,R\}$ ตามลักษณะดังกล่าวเป็นผลให้ เซตของกลุ่มที่ได้ทั้งหมดเป็นผลแบ่งกั้นของ $U_p \backslash \{L,R\}$
จากสมบัติข้อ (i) และ (ii) เราได้ว่า แต่ละกลุ่มประกอบด้วยสับเซต p สับเซต และมีเพียงสับเซตเดียวที่ผลบวกของสมาชิกในสับเซตหารด้วย p ลงตัว
ฉะนั้น จำนวนของกลุ่มทั้งหมดคือจำนวนของสมาชิกในเซต $U_p \backslash \{L,R\} \cap \mathcal{D}_p$
เนื่องจาก $|U_p \backslash \{L,R\}| = \binom{2p}{p} - 2$ ดังนั้น จำนวนของกลุ่มทั้งหมดคือ

$$\frac{1}{p}\left(\binom{2p}{p} - 2\right)$$

จึงได้ว่า

$$|\mathcal{D}_p| = \frac{1}{p}\left(\binom{2p}{p} - 2\right) + 2$$

$\square$

สังเกตเห็นว่า จากบทพิสูจน์ข้างต้น สมบัติข้อ (ii) ยังทำให้เราได้อีกว่า จำนวนของสับเซตที่มีสมาชิก p ตัวของเซต S_{2p} ซึ่งมีสมบัติว่า ผลบวกของสมาชิกในสับเซตสมภาคกับ r มอดุโล p เมื่อ r เป็นจำนวนเต็มซึ่ง $1 \leq r \leq p-1$ คือ

$$\frac{1}{p}\left(\binom{2p}{p} - 2\right)$$

บทแทรก 2.2. ให้ p เป็นจำนวนเฉพาะคี่ใดๆ และ r เป็นจำนวนเต็มซึ่ง $1 \leq r \leq p-1$ จะได้ว่า จำนวนสับเซต A ของเซต S_{2p} ที่มีสมบัติว่า

(i) A มีสมาชิก p ตัว และ

(ii) ผลบวกของสมาชิกในเซต A สมภาคกับ r มอดุโล p

คือ

$$\frac{1}{p}\left(\binom{2p}{p} - 2\right)$$

2.2. ผลเฉลยกรณี p เป็นจำนวนเฉพาะคี่โดยการใช้การกระทำของกรุปบนเซต

ในหัวข้อนี้ เรานำความรู้เรื่องการกระทำของกรุปบนเซตมาประยุกต์กับแนวคิดของบทพิสูจน์ในหัวข้อ 2.1 ได้บทพิสูจน์ที่มีความกระชับขึ้นดังนี้

บทพิสูจน์ของทฤษฎีบท 2.1. .

พิจารณา $\mathbb{Z}_p$ เป็นกรุปภายใต้การบวกมอดุโล p ให้ $\mathbb{Z}_p$ กระทำบนเซต U_p โดย

$$x \cdot A = (x \oplus A_L) \cup A_R$$

เราทราบมาแล้วว่า เซตของวงโคจรที่แตกต่างกันทั้งหมดเป็นผลแบ่งกั้นของ U_p หากเราแสดงได้ว่าแต่ละวงโคจรมีสมาชิกที่ร่วมกันกับ $\mathcal{D}_p$ หนึ่งตัว

$|\mathcal{D}_p|$ คือ จำนวนของวงโคจรที่แตกต่างกันทั้งหมด

เห็นได้ชัดว่า $orb(L) = \{L\}$ และ $orb(R) = \{R\}$ (ได้แสดงไว้ในหัวข้อ 2.1 แล้วว่า L และ R เป็นสมาชิกของ $\mathcal{D}_p$)

พิจารณา

$$orb(A) = \{(x \oplus A_L) \cup A_R \mid x \in \mathbb{Z}_p\} \quad \text{โดยที่} \quad A \in U_p \backslash \{L, R\}$$

เราได้แสดงไว้ในบทพิสูจน์ของทฤษฎีบท 2.1 ในหัวข้อที่ผ่านมาแล้วว่า

$\{(x \oplus A_L) \cup A_R \mid x \in \mathbb{Z}_p\}$ มีสมาชิก p ตัว และ

$\{\sigma((x \oplus A_L) \cup A_R) \mid x \in \mathbb{Z}_p\}$ เป็นระบบส่วนตกค้างบริบูรณ์ มอดุโล p

ฉะนั้น

$orb(A)$ มีสมาชิกที่ร่วมกันกับเซต $\mathcal{D}_p$ หนึ่งตัว และ $|orb(A)| = p$ ทุก $A \in \{U_p \backslash \{L, R\}\}$

ให้ $\mathcal{N}_p$ แทน จำนวนของวงโคจรทั้งหมดที่มีสมาชิก p ตัว จะได้ว่า

$$p \cdot \mathcal{N}_p = |U_p \backslash \{L, R\}| = \binom{2p}{p} - 2$$

ฉะนั้น

$$\mathcal{N}_p = \frac{1}{p}\left(\binom{2p}{p} - 2\right)$$

จึงได้ว่า

$$|\mathcal{D}_p| = \frac{1}{p}\left(\binom{2p}{p} - 2\right) + 2$$

□

หมายเหตุ การเป็นระบบส่วนตกค้างบริบูรณ์ของ $\{\sigma(x \cdot A) \mid x \in \mathbb{Z}_p\}$ ทุก $A \in U_p \backslash \{L, R\}$ จากบทพิสูจน์ข้างต้น ก็เป็นอีกบทพิสูจน์หนึ่งของบทแทรก 2.2

2.3. ผลเฉลยกรณี p เป็นจำนวนเฉพาะคี่โดยการใช้ฟังก์ชันก่อกำเนิดและรากปฐมฐาน . ที่ p ของ 1

เราจะเริ่มต้นหัวข้อนี้ โดยการอธิบายแนวคิดของการใช้เทคนิคของฟังก์ชันก่อกำเนิดมาพิสูจน์ทฤษฎีบท 2.1 ดังนี้

แนวคิด ให้ $c_{r,s}$ แทนจำนวนของสับเซต A ทั้งหมดของเซต S_{2p} ซึ่ง $|A| = r$ และ $\sum\limits_{x\in A} x = s$ หรืออีกนัยหนึ่ง $c_{r,s}$ คือจำนวนวิธีที่เราสามารถเขียน s ให้อยู่ในรูปของผลบวกของจำนวนเต็มบวก r จำนวนซึ่งแตกต่างกันทั้งหมดในเซต S_{2p}

สังเกตเห็นว่า ค่าของ r ที่เป็นไปได้ทั้งหมดคือ $0, 1, \ldots, 2p$ และค่าของ s ที่เป็นไปได้ทั้งหมดคือ $0, 1, \ldots, p(2p+1)$

โดยใช้เทคนิคเดียวกับตัวอย่าง 1.4.3 เราได้ว่า $F(x, y) = \prod\limits_{k=1}^{2p}(1 + xy^k)$ คือฟังก์ชันก่อกำเนิดของแถวลำดับสองชั้น

$$(c_{r,s}) = (c_{0,0}, \ldots, c_{0,p(2p+1)}, c_{1,0}, \ldots, c_{1,p(2p+1)}, \ldots, c_{2p,0}, \ldots, c_{2p,p(2p+1)})$$

ฉะนั้น $|\mathcal{D}_p| = \sum\limits_{\substack{r=p\\ p|s}} c_{r,s}$ เราจึงต้องการพิสูจน์ทฤษฎีบท 2.1 โดยการแสดงว่า

$$\sum_{\substack{r=p\\ p|s}} c_{r,s} = \frac{1}{p}\left(\binom{2p}{p} - 2\right) + 2$$

ซึ่งจะต้องอาศัยทฤษฎีบทประกอบที่เกี่ยวข้องกับรากปฐมฐานที่ p ของ 1 มาเชื่อมโยงกับพหุนาม $\prod\limits_{k=1}^{2p}(1 + xy^k)$

ทฤษฎีบทประกอบที่จะเสนอต่อไปนี้ เรากำหนดโดยพิจารณารากปฐมฐานที่ n เป็นจำนวนเต็มบวกใดๆ ของ 1 เพื่อจะได้ใช้อ้างในบทที่ 3 ต่อไป

ทฤษฎีบทประกอบ 2.3.1. ให้ n เป็นจำนวนเต็มบวกใดๆ และ ζ เป็นรากปฐมฐานที่ n ของ 1 จะได้ว่า สำหรับจำนวนเต็ม $r \geq 0$

$$\sum_{i=0}^{n-1} \zeta^{ri} = \begin{cases} n & \text{ถ้า } n|r \\ 0 & \text{ถ้า } n\nmid r \end{cases}$$

บทพิสูจน์. สมมติว่า $n|r$ จะได้ $\zeta^r = 1$ ดังนั้น $\zeta^{ri} = 1$ ทุก $i \in \{0, 1, \ldots, n-1\}$

จึงได้ว่า

$$\sum_{i=0}^{n-1} \zeta^{ri} = \sum_{i=0}^{n-1} 1 = n \cdot 1 = n$$

สมมติว่า $n \nmid r$ จะได้ว่า $\zeta^r \neq 1$ ดังนั้น $\zeta^r - 1 \neq 0$
เนื่องจาก

$$(\zeta^r - 1)\left(\zeta^{r(n-1)} + \zeta^{r(n-2)} + \ldots + \zeta^r + 1\right) = \zeta^{rn} - 1 = \zeta^n - 1 = 0$$

ดังนั้น $\left(\zeta^{r(n-1)} + \ldots + \zeta^r + 1\right) = 0$ นั่นคือ $\sum_{i=0}^{n-1} \zeta^{ri} = 0$ □

ทฤษฎีบทประกอบ 2.3.2. ให้ n เป็นจำนวนเต็มบวกใดๆ ζ เป็นรากปฐมฐานที่ n ของ 1 และ

$$P(x,y) = \sum_{r,s=0}^{k,m} b_{r,s} x^r y^s$$

เป็นพหุนามใดๆ จะได้ว่า

$$\sum_{i,j=0}^{n-1} P\left(\zeta^i, \zeta^j\right) = n^2 \sum_{\substack{n|r \\ n|s}} b_{r,s}$$

บทพิสูจน์. พิจารณา

$$\begin{aligned}
\sum_{i,j=0}^{n-1} P\left(\zeta^i, \zeta^j\right) &= \sum_{i,j=0}^{n-1} \sum_{r,s=0}^{k,m} b_{r,s} \zeta^{ri} \zeta^{sj} \\
&= \sum_{r,s=0}^{k,m} b_{r,s} \sum_{i,j=0}^{n-1} \zeta^{ri} \zeta^{sj} \\
&= \sum_{\substack{n|r \\ n|s}} b_{r,s} \sum_{i,j=0}^{n-1} \zeta^{ri} \zeta^{sj} + \sum_{\substack{n \nmid r \\ \text{หรือ } n \nmid s}} b_{r,s} \sum_{i,j=0}^{n-1} \zeta^{ri} \zeta^{sj} \qquad (2.1)
\end{aligned}$$

เราจะแบ่งการพิจารณาค่าของ $\sum_{i,j=0}^{n-1} \zeta^{ri} \zeta^{sj}$ ออกเป็น 2 กรณีดังนี้

กรณี 1 $n|r$ และ $n|s$
โดยทฤษฎีบทประกอบ 2.3.1 เราได้ว่า

$$\sum_{i=0}^{n-1} \zeta^{ri} = \sum_{j=0}^{n-1} \zeta^{sj} = n$$

ดังนั้น

$$\begin{aligned}
\sum_{i,j=0}^{n-1} \zeta^{ri} \zeta^{sj} &= \sum_{i=0}^{n-1} \zeta^{ri} \sum_{j=0}^{n-1} \zeta^{sj} \\
&= n \cdot n \\
&= n^2
\end{aligned}$$

กรณี 2 $n \nmid r$ หรือ $n \nmid s$

สมมติ $n \nmid s$ โดยทฤษฎีบทประกอบ 2.3.1 จะได้ว่า $\displaystyle\sum_{j=0}^{n-1} \zeta^{sj} = 0$

ฉะนั้น

$$\begin{aligned}\sum_{i,j=0}^{n-1} \zeta^{ri}\zeta^{sj} &= \sum_{i=0}^{n-1} \zeta^{ri} \sum_{j=0}^{n-1} \zeta^{sj} \\ &= \sum_{i=0}^{n-1} \zeta^{ri} \cdot 0 \\ &= 0\end{aligned}$$

ถ้า $n \nmid r$ ก็สามารถพิสูจน์และให้ผลในทำนองเดียวกัน

จากทั้ง 2 กรณี และ (2.1) เราได้ว่า

$$\begin{aligned}\sum_{i,j=0}^{n-1} P\left(\zeta^i, \zeta^j\right) &= \sum_{\substack{n|r \\ n|s}} b_{r,s} \cdot n^2 + \sum_{\substack{n\nmid r \\ \text{หรือ } n\nmid s}} b_{r,s} \cdot 0 \\ &= n^2 \sum_{\substack{n|r \\ n|s}} b_{r,s}\end{aligned}$$

□

ทฤษฎีบทประกอบ 2.3.3. ให้ n เป็นจำนวนเต็มบวกใดๆ และ ζ เป็นรากปฐมฐานที่ n ของ 1 จะได้ว่า

$$\prod_{k=1}^{n} (1+\zeta^k) = \begin{cases} 2 & \text{ถ้า } n \text{ เป็นจำนวนคี่} \\ 0 & \text{ถ้า } n \text{ เป็นจำนวนคู่}\end{cases}$$

บทพิสูจน์. ให้ ζ เป็นรากปฐมฐานที่ n ของ 1 จะได้ว่า

$$\begin{aligned}\prod_{k=1}^{n} \left(1+\zeta^k\right) &= \prod_{k=1}^{n} (-1)\left(-1-\zeta^k\right) \\ &= (-1)^n \prod_{k=1}^{n} \left(-1-\zeta^k\right) \\ &= (-1)^n \left((-1)^n - 1\right) \qquad \text{(โดยบทแทรก 1.2.5)} \\ &= \begin{cases} 2 & \text{ถ้า } n \text{ เป็นจำนวนคี่} \\ 0 & \text{ถ้า } n \text{ เป็นจำนวนคู่}\end{cases}\end{aligned}$$

□

บทแทรก 2.3.4. ให้ j และ n เป็นจำนวนเต็มบวกซึ่ง $(j,n)=1$ และ ζ เป็นรากปฐมฐานที่ n ของ 1 จะได้ว่า สำหรับจำนวนเต็ม $i \geq 0$

$$\prod_{k=1}^{2n}(1+\zeta^{i+kj}) = \begin{cases} 4 & \text{ถ้า } n \text{ เป็นจำนวนคี่} \\ 0 & \text{ถ้า } n \text{ เป็นจำนวนคู่} \end{cases}$$

บทพิสูจน์. โดยทฤษฎีบท 1.2.6(ii) จะได้ว่า

$$\{\zeta^{i+kj} \mid k=1,2,\ldots,n\} = \{\zeta^{i+kj} \mid k=n+1,n+2,\ldots,2n\}$$

เป็นเซตของรากที่ n ซึ่งแตกต่างกันทั้งหมดของ 1 ทุกจำนวนเต็ม $i \geq 0$
ดังนั้น

$$\begin{aligned}\prod_{k=1}^{2n}\left(1+\zeta^{i+kj}\right) &= \left(\prod_{k=1}^{n}\left(1+\zeta^{i+kj}\right)\right)^2 \\ &= \left(\prod_{k=1}^{n}\left(1+\zeta^{k}\right)\right)^2 \\ &= \begin{cases} 4 & \text{ถ้า } n \text{ เป็นจำนวนคี่} \\ 0 & \text{ถ้า } n \text{ เป็นจำนวนคู่} \end{cases}\end{aligned}$$

(โดยทฤษฎีบทประกอบ 2.3.3)

□

บทพิสูจน์ของทฤษฎีบท 2.1.
ให้

$$F(x,y) = \prod_{k=1}^{2p}\left(1+xy^k\right)$$

เราสามารถเขียน $F(x,y)$ ในอีกรูปแบบได้ดังนี้

$$F(x,y) = 1 + x^{2p}y^{p(2p+1)} + \sum_{r=1}^{2p-1}\sum_{s=1}^{p(2p+1)-1} c_{r,s}x^r y^s$$

โดยทฤษฎีบทประกอบ 2.3.2 จะได้ว่า

$$2 + \sum_{\substack{r=p \\ p|s}} c_{r,s} = \frac{1}{p^2}\sum_{i,j=0}^{p-1} F\left(\zeta^i,\zeta^j\right)$$

ดังนั้น

$$\begin{aligned}|\mathcal{D}_p| = \sum_{\substack{r=p \\ p|s}} c_{r,s} &= \frac{1}{p^2}\sum_{i,j=0}^{p-1} F\left(\zeta^i,\zeta^j\right) - 2 \\ &= \frac{1}{p^2}\sum_{i,j=0}^{p-1}\prod_{k=1}^{2p}\left(1+\zeta^{i+kj}\right) - 2 \qquad (2.2)\end{aligned}$$

ต่อไปจะหาค่าของ $\sum_{i,j=0}^{p-1}\prod_{k=1}^{2p}\left(1+\zeta^{i+kj}\right)$

โดยบทแทรก 2.3.4 จะได้ว่า

$$\begin{aligned}\sum_{i,j=0}^{p-1}\prod_{k=1}^{2p}\left(1+\zeta^{i+kj}\right) &= \sum_{i=0}^{p-1}\prod_{k=1}^{2p}\left(1+\zeta^{i}\right)+\sum_{i=0}^{p-1}\sum_{j=1}^{p-1}\prod_{k=1}^{2p}\left(1+\zeta^{i+kj}\right)\\ &= \sum_{i=0}^{p-1}\left(1+\zeta^{i}\right)^{2p}+4(p-1)p \qquad (2.3)\end{aligned}$$

พิจารณา

$$\begin{aligned}\sum_{i=0}^{p-1}\left(1+\zeta^{i}\right)^{2p} &= \sum_{i=0}^{p-1}\sum_{k=0}^{2p}\binom{2p}{k}\zeta^{ik}\\ &= \sum_{k=0}^{2p}\binom{2p}{k}\sum_{i=0}^{p-1}\zeta^{ik}\\ &= \binom{2p}{0}p+\binom{2p}{p}p+\binom{2p}{2p}p\\ &\qquad \text{(โดยทฤษฎีบทประกอบ 2.3.1)}\\ &= p\left(2+\binom{2p}{p}\right) \qquad (2.4)\end{aligned}$$

จาก (2.2),(2.3) และ (2.4) จะได้ว่า

$$\begin{aligned}|\mathcal{D}_p| &= \frac{1}{p^2}\left(p\left(2+\binom{2p}{p}\right)+4(p-1)p\right)-2\\ &= \frac{1}{p}\left(\binom{2p}{p}-2\right)+2\end{aligned}$$

□

2.4. ผลเฉลยกรณี p เป็นจำนวนเฉพาะคี่โดยการผสมผสานความรู้ทางพีชคณิตนามธรรม ทฤษฎีจำนวน และคอมบินาทอริค

บทพิสูจน์ของทฤษฎีบท 2.1 ที่จะเสนอต่อไปนี้ ค้นพบโดยผู้นำทีมจากประเทศอิตาลี ความสวยงามของบทพิสูจน์นี้ เกิดจากการผสมผสานที่ลงตัวของความรู้ทางพีชคณิตนามธรรม ทฤษฎีจำนวน และคอมบินาทอริค

บทพิสูจน์ของทฤษฎีบท 2.1.

พิจารณาพหุนาม

$$\prod_{i=1}^{2p}\left(x-\zeta^{i}\right)$$

หากเรากระจาย $\prod_{i=1}^{2p}\left(x-\zeta^{i}\right)$ ให้อยู่ในรูปผลบวกของเอกนาม จะได้ว่า สัมประสิทธิ์ของ x^p ก็คือ

$$\sum_{\{i_1,\ldots,i_p\}\subseteq S_{2p}} (-1)^p \zeta^{i_1+\ldots+i_p} = -\sum_{j=0}^{p-1} n_j \zeta^j \tag{2.5}$$

เมื่อ n_j แทน จำนวนของสับเซต $\{i_1, i_2, \ldots, i_p\}$ ของเซต S_{2p} ซึ่ง

$$i_1 + i_2 + \ldots + i_p \equiv j \pmod{p}$$

สังเกตเห็นว่า $|\mathcal{D}_p| = n_0$
ในการพิสูจน์ทฤษฎีบทเราต้องการหาค่าของ n_0
เนื่องจาก

$$\prod_{i=1}^{2p}\left(x-\zeta^{i}\right) = \left(x^p - 1\right)^2 = x^{2p} - 2x^p + 1$$

ดังนั้น เราได้โดย (2.5) ว่า

$$\sum_{j=0}^{p-1} n_j \zeta^j = 2$$

ทำให้

$$n_0 - 2 + \sum_{j=1}^{p-1} n_j \zeta^j = 0$$

จึงได้ว่า ζ เป็นรากของพหุนาม $n_0 - 2 + \sum_{j=1}^{p-1} n_j x^j$
โดยทฤษฎีบท 1.2.10 เราได้ว่า $1 + x + \ldots + x^{p-1}$ เป็นพหุนามเล็กสุดเฉพาะกลุ่มของ ζ บน $\mathbb{Q}$
ฉะนั้น

$$n_0 - 2 + \sum_{j=1}^{p-1} n_j x^j = k \cdot \left(1 + x + \ldots + x^{p-1}\right) \quad \text{โดยที่} \quad k \in \mathbb{Q}$$

โดยการเทียบสัมประสิทธิ์ของสมการ เราได้ว่า

$$n_0 = k + 2 \quad \text{และ}$$
$$n_j = k \quad \text{ทุก} \quad j \in \{1, 2, \ldots, p-1\}$$

ดังนั้น

$$2 + p \cdot k = \sum_{j=0}^{p-1} n_j = \binom{2p}{p}$$

ทำให้ได้ว่า

$$k = \frac{1}{p}\left(\binom{2p}{p} - 2\right)$$

เพราะฉะนั้น

$$|\mathcal{D}_p| = \frac{1}{p}\left(\binom{2p}{p} - 2\right) + 2$$

ยิ่งกว่านั้น ค่าของ $n_j = \frac{1}{p}\left(\binom{2p}{p} - 2\right)$ ทุก $j \in \{1, 2, \ldots, p-1\}$ ก็เป็นอีกบทพิสูจน์หนึ่งของบทแทรก 2.2 $\square$

บทที่ 3

ผลเฉลยกรณี n เป็นจำนวนเต็มบวกใดๆ

เราได้ขยายขอบเขตของปัญหาเพื่อศึกษาจำนวนของสับเซตที่มีสมาชิก n ตัวของเซต S_{2n} ซึ่งมีสมบัติว่า ผลบวกของสมาชิกในสับเซตหารด้วย n ลงตัว โดยที่ n เป็นจำนวนเต็มบวกใดๆ จากการศึกษาพบว่า กระบวนการนับจำนวนของสับเซตดังกล่าวมีความซับซ้อนมากขึ้น ซึ่งต้องอาศัยทฤษฎีบทประกอบเพิ่มเติมดังต่อไปนี้

ทฤษฎีบทประกอบ 3.1. ให้ n เป็นจำนวนเต็มบวกใดๆ และ ζ เป็นรากปฐมฐานที่ n ของ 1 จะได้ว่า

$$\prod_{k=1}^{n} \zeta^k = \begin{cases} 1 & \text{ถ้า } n \text{ เป็นจำนวนคี่} \\ -1 & \text{ถ้า } n \text{ เป็นจำนวนคู่} \end{cases}$$

บทพิสูจน์. พิจารณา

$$\zeta^k \cdot \zeta^{n-k} = \zeta^n = 1 \quad \text{เมื่อ } k \text{ เป็นจำนวนเต็มซึ่ง } 1 \le k \le n-1$$

ถ้า n เป็นจำนวนคี่ จะได้ว่า

$$\prod_{k=1}^{n} \zeta^k = 1 \cdot \prod_{k=1}^{n-1} \zeta^k = \prod_{k=1}^{(n-1)/2} \zeta^k \zeta^{n-k} = \prod_{k=1}^{(n-1)/2} 1 = 1$$

ถ้า n เป็นจำนวนคู่ จะได้ว่า

$$\prod_{k=1}^{n} \zeta^k = 1 \cdot \prod_{k=1}^{n-1} \zeta^k = \zeta^{\frac{n}{2}} \cdot \prod_{k=1}^{(n/2)-1} \zeta^k \zeta^{n-k} = \zeta^{\frac{n}{2}} = -1 \quad \text{(โดยทฤษฎีบท 1.2.8 (i))}$$

□

ทฤษฎีบทประกอบ 3.2. ให้ d และ n เป็นจำนวนเต็มบวกซึ่ง $d|n$ และ ζ เป็นรากปฐมฐานที่ n ของ 1 จะได้ว่า สำหรับแต่ละจำนวนเต็ม $i \ge 0$

$$\prod_{k=1}^{n/d} \left(1 + \zeta^{i+kd}\right) = \begin{cases} 1 + \zeta^{i(n/d)} & \text{ถ้า } \frac{n}{d} \text{ เป็นจำนวนคี่} \\ 1 - \zeta^{i(n/d)} & \text{ถ้า } \frac{n}{d} \text{ เป็นจำนวนคู่} \end{cases}$$

บทพิสูจน์. โดยทฤษฎีบท 1.2.8 (ii) เราได้ว่า ζ^d เป็นรากปฐมฐานที่ $\frac{n}{d}$ ของ 1

พิจารณา

$$\begin{aligned}\prod_{k=1}^{n/d}\left(\zeta^{d}\right)^{k}\prod_{k=1}^{n/d}\left(1+\zeta^{i+kd}\right) &= \prod_{k=1}^{n/d}\left(\zeta^{d}\right)^{(n/d)-k}\prod_{k=1}^{n/d}\left(1+\zeta^{i+kd}\right)\\ &= \prod_{k=1}^{n/d}\zeta^{n-kd}\prod_{k=1}^{n/d}\left(1+\zeta^{i+kd}\right)\\ &= \prod_{k=1}^{n/d}\left(\zeta^{n-kd}+\zeta^{(n-kd)+(i+kd)}\right)\\ &= \prod_{k=1}^{n/d}\left(\left(\zeta^{d}\right)^{(n/d)-k}+\zeta^{i}\right)\\ &= \prod_{k=1}^{n/d}\left(\left(\zeta^{d}\right)^{k}+\zeta^{i}\right) \qquad (3.1)\end{aligned}$$

กรณี $\frac{n}{d}$ เป็นจำนวนคี่ จะได้ว่า

$$\begin{aligned}1\cdot\prod_{k=1}^{n/d}\left(1+\zeta^{i+kd}\right) &= \prod_{k=1}^{n/d}\left(\zeta^{d}\right)^{k}\prod_{k=1}^{n/d}\left(1+\zeta^{i+kd}\right) \quad \text{(โดยทฤษฎีบทประกอบ 3.1)}\\ &= \prod_{k=1}^{n/d}\left(\left(\zeta^{d}\right)^{k}+\zeta^{i}\right) \quad \text{(โดย(3.1))}\\ &= \left(\zeta^{i}\right)^{n/d}+1 \quad \text{(โดยทฤษฎีบท 1.2.7)}\end{aligned}$$

นั่นคือ $\prod_{k=1}^{n/d}\left(1+\zeta^{i+kd}\right)=1+\zeta^{i(n/d)}$

กรณี $\frac{n}{d}$ เป็นจำนวนคู่ จะได้ว่า

$$\begin{aligned}1\cdot(-1)\cdot\prod_{k=1}^{n/d}\left(1+\zeta^{i+kd}\right) &= \left(\left(\zeta^{d}\right)^{\frac{n/d}{2}}\right)^{n/d}\prod_{k=1}^{n/d}\left(\zeta^{d}\right)^{k}\prod_{k=1}^{n/d}\left(1+\zeta^{i+kd}\right)\\ &\qquad \text{(โดยทฤษฎีบท 1.2.8(i) และทฤษฎีบทประกอบ 3.1)}\\ &= \left(\left(\zeta^{d}\right)^{\frac{n/d}{2}}\right)^{n/d}\prod_{k=1}^{n/d}\left(\left(\zeta^{d}\right)^{k}+\zeta^{i}\right) \quad \text{(โดย (3.1))}\\ &= \prod_{k=1}^{n/d}\left(\left(\zeta^{d}\right)^{\frac{n/d}{2}+k}-\zeta^{i}\right)\\ &= \prod_{k=1}^{n/d}\left(\left(\zeta^{d}\right)^{k}-\zeta^{i}\right) \quad \text{(โดยทฤษฎีบท 1.2.6 (ii))}\\ &= \left(\zeta^{i}\right)^{n/d}-1 \quad \text{(โดยบทแทรก 1.2.5)}\end{aligned}$$

นั่นคือ $\prod_{k=1}^{n/d}\left(1+\zeta^{i+kd}\right)=1-\zeta^{i(n/d)}$ □

ทฤษฎีบท 3.3. ให้ n เป็นจำนวนเต็มบวกใดๆ และ ζ เป็นรากปฐมฐานที่ n ของ 1 จะได้ว่า สำหรับจำนวนเต็ม $i \geq 0$

$$\sum_{\substack{j=1 \\ (j,n)\neq 1}}^{n} \prod_{k=1}^{2n} \left(1+\zeta^{i+kj}\right) = \sum_{\substack{d\neq 1 \\ d|n}} \phi\left(\frac{n}{d}\right) \left(\prod_{k=1}^{n/d} \left(1+\zeta^{i+kd}\right)\right)^{2d}$$

บทพิสูจน์. สำหรับจำนวนเต็มบวก d, j และ n ใดๆ จะได้ว่า

$$(j,n) = d \text{ ก็ต่อเมื่อ } \left(\frac{j}{d}, \frac{n}{d}\right) = 1$$

ฉะนั้น

$$|\{j \in \mathbb{N} \mid j \leq n \text{ และ } (j,n) = d\}| = \phi\left(\frac{n}{d}\right)$$

จึงเพียงพอที่จะพิสูจน์ทฤษฎีบทโดยการแสดงว่า สำหรับแต่ละ $j \in \{1, 2, \ldots, n\}$
ถ้า $(j,n) = d$ แล้ว

$$\prod_{k=1}^{2n} \left(1+\zeta^{i+kj}\right) = \left(\prod_{k=1}^{n/d} \left(1+\zeta^{i+kd}\right)\right)^{2d}$$

ให้ $(j,n) = d$ โดยทฤษฎีบท 1.2.8 (iii) เราได้ว่า ζ^j เป็นรากปฐมฐานที่ $\frac{n}{d}$ ของ 1 ดังนั้น

$$\left\{\zeta^{kj} \mid k = \frac{ln}{d}+1, \frac{ln}{d}+2, \ldots, \frac{ln}{d}+\frac{n}{d}\right\} = \left\{\zeta^{kd} \mid k = 1, 2, \ldots, \frac{n}{d}\right\}$$

เป็นเซตของรากที่ $\frac{n}{d}$ ซึ่งแตกต่างกันทั้งหมดของ 1 ทุกจำนวนเต็ม $l \geq 0$

จึงได้ว่า

$$\left\{1+\zeta^{i+kj} \mid k = \frac{ln}{d}+1, \frac{ln}{d}+2, \ldots, \frac{ln}{d}+\frac{n}{d}\right\} = \left\{1+\zeta^{i+kd} \mid k = 1, 2, \ldots, \frac{n}{d}\right\}$$

ทุกจำนวนเต็ม $l \geq 0$
ดังนั้น

$$\begin{aligned} \prod_{k=1}^{2n} \left(1+\zeta^{i+kj}\right) &= \left(\prod_{k=1}^{n/d} \left(1+\zeta^{i+kd}\right)\right)^{\frac{2n}{n/d}} \\ &= \left(\prod_{k=1}^{n/d} \left(1+\zeta^{i+kd}\right)\right)^{2d} \end{aligned}$$

□

ต่อไปจะเสนอโจทย์ปัญหาและผลเฉลย ซึ่งขยายจากกรณีจำนวนเฉพาะคี่ p ไปยังกรณีจำนวนเต็มบวก n ใดๆ ในรูปแบบทฤษฎีบทดังนี้

ทฤษฎีบท 3.4. ให้ n เป็นจำนวนเต็มบวกใดๆ จะได้ว่า จำนวนของสับเซต A ของเซต S_{2n} ซึ่งมีสมบัติว่า

(i) A มีสมาชิก n ตัว และ

(ii) ผลบวกของสมาชิกในเซต A หารด้วย n ลงตัว

คือ

$$\frac{(-1)^n}{n}\sum_{d|n}\phi\left(\frac{n}{d}\right)\binom{2d}{d}(-1)^d$$

หรืออีกนัยหนึ่ง ถ้าเราให้ $\mathcal{D}_n = \left\{ A \subseteq S_{2n} \mid |A| = n \text{ และ } n \mid \sum_{x\in A} x \right\}$ แล้ว

$$|\mathcal{D}_n| = \frac{(-1)^n}{n}\sum_{d|n}\phi\left(\frac{n}{d}\right)\binom{2d}{d}(-1)^d$$

แนวคิด ได้จากการพิจารณาวิธีแก้ปัญหากรณีจำนวนเฉพาะคี่ p โดยการใช้เทคนิคของฟังก์ชันก่อกำเนิดและรากปฐมฐานที่ p ของ 1
เนื่องจาก

$$F(x,y) = \prod_{k=1}^{2n}(1+xy^k) = 1 + x^{2n}y^{n(2n+1)} + \sum_{r=1}^{2n-1}\sum_{s=1}^{n(2n+1)-1} c_{r,s}x^r y^s \tag{3.2}$$

คือฟังก์ชันก่อกำเนิดของแถวลำดับสองชั้น

$$(c_{r,s}) = (c_{0,0}, \ldots, c_{0,n(2n+1)}, c_{1,0}, \ldots, c_{1,n(2n+1)}, \ldots, c_{2n,0}, \ldots, c_{2n,n(2n+1)})$$

เมื่อ $c_{r,s}$ คือ จำนวนของสับเซต A ทั้งหมดของเซต S_{2n} ที่ $|A| = r$ และ $\sum_{x\in A} x = s$

และเนื่องจาก $|\mathcal{D}_n| = \sum_{\substack{r=n\\ n|s}} c_{r,s}$

ดังนั้นเราจะพิสูจน์ทฤษฎีบท 3.4 โดยอาศัยทฤษฎีบทและทฤษฎีบทประกอบทั้งหลายก่อนหน้านี้ หาค่าของ $\sum_{\substack{r=n\\ n|s}} c_{r,s}$ ดังนี้

บทพิสูจน์. ให้ ζ เป็นรากปฐมฐานที่ n ของ 1 และ

$$F(x,y) = \prod_{k=1}^{2n}\left(1+xy^k\right)$$

จาก (3.2) และทฤษฎีบทประกอบ 2.3.2 จะได้ว่า

$$|\mathcal{D}_n| = \sum_{\substack{r=n \\ n|s}} c_{r,s} = \frac{1}{n^2}\sum_{i,j=0}^{n-1} F(\zeta^i,\zeta^j) - 2$$

$$= \frac{1}{n^2}\sum_{i,j=0}^{n-1}\prod_{k=1}^{2n}\left(1+\zeta^{i+kj}\right) - 2 \tag{3.3}$$

เราจะแบ่งการพิจารณาค่าของ $\sum\limits_{i,j=0}^{n-1}\prod\limits_{k=1}^{2n}(1+\zeta^{i+kj})$ ออกเป็น 2 กรณีดังนี้

กรณี 1 n เป็นจำนวนคู่ จะได้ว่า

$$\sum_{i,j=0}^{n-1}\prod_{k=1}^{2n}\left(1+\zeta^{i+kj}\right) = \sum_{i=0}^{n-1}\sum_{\substack{j=1 \\ (j,n)\neq 1}}^{n}\prod_{k=1}^{2n}\left(1+\zeta^{i+kj}\right)$$

(โดยบทแทรก 2.3.4)

$$= \sum_{i=0}^{n-1}\sum_{\substack{d\neq 1 \\ d|n}}\phi\left(\frac{n}{d}\right)\left(\prod_{k=1}^{n/d}\left(1+\zeta^{i+kd}\right)\right)^{2d}$$

(โดยทฤษฎีบท 3.3)

$$= \sum_{i=0}^{n-1}\sum_{\substack{d\neq 1 \\ (n/d)\in\mathbb{E}}}\phi\left(\frac{n}{d}\right)\left(1-\zeta^{i(n/d)}\right)^{2d}$$

$$+\sum_{i=0}^{n-1}\sum_{\substack{d\neq 1 \\ (n/d)\in\mathbb{O}}}\phi\left(\frac{n}{d}\right)\left(1+\zeta^{i(n/d)}\right)^{2d} \tag{3.4}$$

(โดยทฤษฎีบทประกอบ 3.2)

กรณีย่อย 1.1 พิจารณาค่าของ $\displaystyle\sum_{i=0}^{n-1} \sum_{\substack{d \neq 1 \\ (n/d) \in \mathbb{E}}} \phi\left(\frac{n}{d}\right)\left(1-\zeta^{i(n/d)}\right)^{2d}$ จะได้ว่า

$$\begin{aligned}
\sum_{i=0}^{n-1} \sum_{\substack{d \neq 1 \\ (n/d) \in \mathbb{E}}} \phi\left(\frac{n}{d}\right)\left(1-\zeta^{i(n/d)}\right)^{2d} &= \sum_{i=0}^{n-1} \sum_{\substack{d \neq 1 \\ (n/d) \in \mathbb{E}}} \phi\left(\frac{n}{d}\right) \sum_{k=0}^{2d} \binom{2d}{k}(-1)^k \zeta^{i(n/d)k} \\
&= \sum_{\substack{d \neq 1 \\ (n/d) \in \mathbb{E}}} \phi\left(\frac{n}{d}\right) \sum_{k=0}^{2d} \binom{2d}{k}(-1)^k \sum_{i=0}^{n-1} \zeta^{i(n/d)k} \\
&= \sum_{\substack{d \neq 1 \\ (n/d) \in \mathbb{E}}} \phi\left(\frac{n}{d}\right)\left(\binom{2d}{0}(-1)^0 n+\binom{2d}{d}(-1)^d n+\binom{2d}{2d}(-1)^{2d} n\right)
\end{aligned}$$

(โดยทฤษฎีบทประกอบ 2.3.1)

$$= n \sum_{\substack{d \neq 1 \\ (n/d) \in \mathbb{E}}} \phi\left(\frac{n}{d}\right)\left(2+\binom{2d}{d}(-1)^d\right) \tag{3.5}$$

กรณีย่อย 1.2 พิจารณาค่าของ $\displaystyle\sum_{i=0}^{n-1} \sum_{\substack{d \neq 1 \\ (n/d) \in \mathbb{O}}} \phi\left(\frac{n}{d}\right)\left(1+\zeta^{i(n/d)}\right)^{2d}$ จะได้ว่า

$$\begin{aligned}
\sum_{i=0}^{n-1} \sum_{\substack{d \neq 1 \\ (n/d) \in \mathbb{O}}} \phi\left(\frac{n}{d}\right)\left(1+\zeta^{i(n/d)}\right)^{2d} &= \sum_{i=0}^{n-1} \sum_{\substack{d \neq 1 \\ (n/d) \in \mathbb{O}}} \phi\left(\frac{n}{d}\right) \sum_{k=0}^{2d} \binom{2d}{k} \zeta^{i(n/d)k} \\
&= \sum_{\substack{d \neq 1 \\ (n/d) \in \mathbb{O}}} \phi\left(\frac{n}{d}\right) \sum_{k=0}^{2d} \binom{2d}{k} \sum_{i=0}^{n-1} \zeta^{i(n/d)k} \\
&= \sum_{\substack{d \neq 1 \\ (n/d) \in \mathbb{O}}} \phi\left(\frac{n}{d}\right)\left(\binom{2d}{0} n+\binom{2d}{d} n+\binom{2d}{2d} n\right)
\end{aligned}$$

(โดยทฤษฎีบทประกอบ 2.3.1)

$$\begin{aligned}
&= n \sum_{\substack{d \neq 1 \\ (n/d) \in \mathbb{O}}} \phi\left(\frac{n}{d}\right)\left(2+\binom{2d}{d}\right) \\
&= n \sum_{\substack{d \neq 1 \\ (n/d) \in \mathbb{O}}} \phi\left(\frac{n}{d}\right)\left(2+\binom{2d}{d}(-1)^d\right) \qquad (3.6)
\end{aligned}$$

(เนื่องจาก $n \in \mathbb{E}$ ดังนั้น ถ้า $d \mid n$ และ $\dfrac{n}{d} \in \mathbb{O}$ แล้ว $d \in \mathbb{E}$)

เราจะได้โดย (3.3),(3.4),(3.5) และ (3.6) ว่า

$$
\begin{aligned}
|\mathcal{D}_n| &= \frac{1}{n^2}\left(n \sum_{\substack{d\neq 1\\ (n/d)\in\mathbb{E}}} \phi\left(\frac{n}{d}\right)\left(2+\binom{2d}{d}(-1)^d\right) + n \sum_{\substack{d\neq 1\\ (n/d)\in\mathbb{O}}} \phi\left(\frac{n}{d}\right)\left(2+\binom{2d}{d}(-1)^d\right)\right) - 2 \\
&= \frac{1}{n}\sum_{\substack{d\neq 1\\ d|n}} \phi\left(\frac{n}{d}\right)\left(2+\binom{2d}{d}(-1)^d\right) - 2 \\
&= \frac{1}{n}\left(\left(\sum_{\substack{d\neq 1\\ d|n}} \phi\left(\frac{n}{d}\right) - n\right) 2 + \sum_{\substack{d\neq 1\\ d|n}} \phi\left(\frac{n}{d}\right)\binom{2d}{d}(-1)^d\right) \\
&= \frac{1}{n}\left(\phi(n)\binom{2}{1}(-1) + \sum_{\substack{d\neq 1\\ d|n}} \phi\left(\frac{n}{d}\right)\binom{2d}{d}(-1)^d\right) \\
&= \frac{1}{n}\sum_{d|n} \phi\left(\frac{n}{d}\right)\binom{2d}{d}(-1)^d
\end{aligned}
$$

กรณี 2 n เป็นจำนวนคี่ จะได้ว่า

$$
\sum_{i,j=0}^{n-1}\prod_{k=1}^{2n}\left(1+\zeta^{i+kj}\right) = \sum_{i=0}^{n-1}\sum_{\substack{j=1\\ (j,n)=1}}^{n} 4 + \sum_{i=0}^{n-1}\sum_{\substack{j=1\\ (j,n)\neq 1}}^{n}\prod_{k=1}^{2n}\left(1+\zeta^{i+kj}\right)
$$

(โดยบทแทรก 2.3.4)

$$
= 4n\phi(n) + \sum_{i=0}^{n-1}\sum_{\substack{d\neq 1\\ d|n}} \phi\left(\frac{n}{d}\right)\left(\prod_{k=1}^{n/d}\left(1+\zeta^{i+kd}\right)\right)^{2d}
$$

(โดยทฤษฎีบท 3.3)

$$
= 4n\phi(n) + \sum_{i=0}^{n-1}\sum_{\substack{d\neq 1\\ d|n}} \phi\left(\frac{n}{d}\right)\left(1+\zeta^{i(n/d)}\right)^{2d}
$$

(เนื่องจาก $n\in\mathbb{O}$ ฉะนั้น ถ้า $d|n$ แล้ว $d\in\mathbb{O}$ ทำให้ $\frac{n}{d}\in\mathbb{O}$ และโดยทฤษฎีบทประกอบ 3.2)

$$
= 4n\phi(n) + n\sum_{\substack{d\neq 1\\ d|n}} \phi\left(\frac{n}{d}\right)\left(2+\binom{2d}{d}\right) \tag{3.7}
$$

(โดยกระบวนการเดียวกันกับกรณี 1)

จาก (3.3) และ (3.7) จะได้ว่า

$$
\begin{aligned}
|\mathcal{D}_n| &= \frac{1}{n^2}\left(4n\phi(n) + n\sum_{\substack{d\neq 1\\ d|n}} \phi\left(\frac{n}{d}\right)\left(2+\binom{2d}{d}\right)\right) - 2\\
&= \frac{1}{n}\left(4\phi(n) + \left(\sum_{\substack{d\neq 1\\ d|n}} \phi\left(\frac{n}{d}\right) - n\right)2 + \sum_{\substack{d\neq 1\\ d|n}} \phi\left(\frac{n}{d}\right)\binom{2d}{d}\right)\\
&= \frac{1}{n}\left(4\phi(n) - 2\phi(n) + \sum_{\substack{d\neq 1\\ d|n}} \phi\left(\frac{n}{d}\right)\binom{2d}{d}\right)\\
&= \frac{1}{n}\sum_{d|n} \phi\left(\frac{n}{d}\right)\binom{2d}{d}
\end{aligned}
$$

จากทั้ง 2 กรณี เราจะได้สูตรทั่วไปของ $\mathcal{D}_n$ คือ

$$
|\mathcal{D}_n| = \frac{(-1)^n}{n}\sum_{d|n} \phi\left(\frac{n}{d}\right)\binom{2d}{d}(-1)^d
$$

$\square$

ข้อสังเกต ค่าของ $|\mathcal{D}_n|$ ในทฤษฎีบท 3.4 เป็นจำนวนเต็มบวกเสมอ

กรณี n เป็นจำนวนคี่ จะได้ว่า จำนวนเต็มบวก d ที่ $d|n$ จะต้องเป็นจำนวนคี่เท่านั้น ฉะนั้น $(-1)^d = -1$ ทุกจำนวนเต็มบวก d ซึ่ง $d|n$ เนื่องจาก $(-1)^n = -1$ ดังนั้น

$$
|\mathcal{D}_n| = \frac{1}{n}\sum_{d|n} \phi\left(\frac{n}{d}\right)\binom{2d}{d} > 0
$$

กรณี n เป็นจำนวนคู่ แม้ว่าจำนวนเต็มบวก d ที่ $d|n$ เป็นได้ทั้งจำนวนคู่และจำนวนคี่ แต่ถ้า d เป็นจำนวนคี่เราได้ว่า $2d|n$

เนื่องจาก $\phi\left(\frac{n}{d}\right)\binom{2d}{d} < \phi\left(\frac{n}{2d}\right)\binom{4d}{2d}$

ดังนั้น $\phi\left(\frac{n}{d}\right)\binom{2d}{d}(-1)^d + \phi\left(\frac{n}{2d}\right)\binom{4d}{2d}(-1)^{2d} > 0$

จึงได้ว่า

$$
|\mathcal{D}_n| = \frac{1}{n}\sum_{d|n} \phi\left(\frac{n}{d}\right)\binom{2d}{d}(-1)^d > 0
$$

ตัวอย่างต่อไปนี้ เป็นการแสดงการใช้ทฤษฎีบท 3.4 หาจำนวนสมาชิกของ $\mathcal{D}_4$

ตัวอย่าง 3.5. โดยทฤษฎีบท 3.4 จะได้ว่า

$$
\begin{aligned}
|\mathcal{D}_4| &= \frac{(-1)^4}{4} \sum_{d|4} \phi\left(\frac{n}{d}\right) \binom{2d}{d} (-1)^d \\
&= \frac{1}{4}\left(\phi(4)\binom{2}{1}(-1) + \phi(2)\binom{4}{2} + \phi(1)\binom{8}{4}\right) \\
&= 18
\end{aligned}
$$

ซึ่งเราสามารถหาสมาชิก 18 ตัวของเซต $\mathcal{D}_4$ ได้ดังนี้

$$
\begin{array}{cccccc}
\{1,2,3,6\} & \{1,2,4,5\} & \{1,2,5,8\} & \{1,2,6,7\} & \{1,3,4,8\} & \{1,3,5,7\} \\
\{1,4,5,6\} & \{1,4,7,8\} & \{1,5,6,8\} & \{2,3,4,7\} & \{2,3,5,6\} & \{2,3,7,8\} \\
\{2,4,6,8\} & \{2,5,6,7\} & \{3,4,5,8\} & \{3,4,6,7\} & \{3,6,7,8\} & \{4,5,7,8\}
\end{array}
$$

รายการอ้างอิง

[1] Greenleaf, F. P. Introduction to Complex Variables. London: W. B. Saunders Com., 1972.

[2] Hungerford, T. W. Algebra. New York: Springer-Verlag, 1994.

[3] Morandi, P. Field and Galois Theory. New York: Springer-Verlag, 1996.

[4] Rosen, K. H. Elementary Number Theory and Its Applications. New York: Addisson-Wesley, 1978.

[5] Stewart, I. N. and Tall, D. O. Algebraic Number Theory. New York: John Wiley & Sons, 1979.

[6] Tucker, A. Applied Combinatorics. 2nd ed. New York: John Wiley & Sons, 1984.

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวศิริญญา โปร่งจิตร์ เกิดที่กรุงเทพฯ เมื่อวันที่ 5 เดือนกันยายน พ.ศ. 2519 จบการศึกษาระดับปริญญาตรีจากภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่นเมื่อ พ.ศ. 2542 เข้าศึกษาต่อระดับปริญญาโทในสาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัยเมื่อปีการศึกษา 2542