ยุทธศาสตร์ กลยุทธ์ และ พื้นฐาน ในการแก้ปัญหาทฤษฎีจำนวน

ผศ. ดร. อรชุน ไชยเสนะ
สาขาวิชาคณิตศาสตร์
สำนักวิชาวิทยาศาสตร์
มหาวิทยาลัยเทคโนโลยีสุรนารี

10 มีนาคม พ.ศ. 2547

1 ทบทวนภาคแรก

ถ้า a/b เป็นจำนวนเต็ม เรากล่าวว่า b หาร a ลงตัว **หรือ** b เป็นตัวประกอบ **หรือ** ตัวหารของ a เราใช้สัญกรณ์ $b \setminus a$ นอกจากนี้ เรากล่าวได้ว่า มีจำนวนเต็ม m ซึ่ง $a = bm$

1.1 *ทฤษฎีบทมูลฐานของเลขคณิต*

ตัวเลข n เป็น **จำนวนเฉพาะ** ถ้ามันไม่มีตัวหารอื่นๆ นอกจาก 1 และตัวมันเอง ถ้าไม่เป็นเช่นนั้น เราเรียก n ว่า เป็นจำนวนประกอบ โดยเป็นที่ตกลงกันว่า 1 ไม่เป็นจำนวนเฉพาะ หรือ ประกอบ ดังนั้นเซทจำนวนเฉพาะจึงเริ่มต้นด้วย

$$2, 3, 5, 7, 11, 13, 17, 23, 29, 31, \ldots$$

แต่ก็ไม่ชัดเจนว่า ลำดับนี้สิ้นสุดหรือไม่

ทฤษฎีบท 1.1 *จำนวนเฉพาะย่อมมีจำนวนเป็นอนันต์*

การพิสูจน์

ในการพิสูจน์ข้างบน เราได้สมมุติว่า Q จะต้องมีอย่างน้อยหนึ่งตัวประกอบ ซึ่งเป็นจำนวนเฉพาะ เราอาจพิสูจน์ได้ว่า ทุกจำนวนเต็มบวกที่มีค่ามากกว่า 1 อาจแยกเป็นผลคูณของจำนวนเฉพาะได้ อาทิ $360 =$

การที่เราสามารถแยกตัวประกอบได้เช่นนี้ เรียกว่า ทฤษฎีบทมูลฐานของเลขคณิต (ทมล) (Fundamental Theorem of Arithmetic) (FTA) และการจัดกลุ่มตัวประกอบเป็นจำนวนเฉพาะเรียกว่า การแยกตัวประกอบเป็นกำลังจำนวนเฉพาะ (prime-power factorization) (PPF) โดยมีสัญกรณ์เช่น

$$n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

ตัวอย่าง 1.1 *ให้* x, y *เป็นจำนวนเต็มซึ่ง* $5x = 3y$ *แล้ว* $3 \setminus x$ *และ* $5 \setminus y$.

การพิสูจน์

ซึ่งเป็นการใช้ FTA ในการพิสูจน์

1.2 GCD, LCM และขั้นตอนวิธีหาร

เมื่อมีจำนวนเต็มบวกสองจำนวน a, b *ตัวหารร่วมมาก* จะเป็นจำนวนเต็มที่ใหญ่ที่สุด ซึ่งหารทั้ง a และ b ลงตัว โดยใช้สัญกรณ์ (a, b) หรือ $GCD(a, b)$

ตัวอย่าง 1.2 *จงหา* $(66, 150)$ *และ* $(100, 250)$

ถ้า $(m,n)=1$ แล้ว เรากล่าวว่า m และ n นั้น เฉพาะสัมพัทธ์ ตัวอย่างเช่น $(p,q)=1$ ถ้า p และ q ต่างเป็นจำนวนเฉพาะ เราจะใช้สัญกรณ์ $a \perp b$ แทน $(a,b)=1$ นอกจากนี้ เรานิยาม ตัวคูณร่วมน้อย หรือ **LCM** ของ a และ b ให้เป็นจำนวนเต็มที่น้อยที่สุดซึ่งเป็นพหุคูณของทั้ง a และ b โดยใช้สัญกรณ์ $[a,b]$ หรือ $LCM(a,b)$

ข้อเท็จจริงที่สำคัญเกี่ยวกับเรื่อง หรม. และ ครน.

1. $a \perp b$ สมมูลกับการกล่าวว่า a และ b ไม่มีจำนวนเฉพาะที่เหมือนกันเลยใน PPF ของมัน

2. ถ้า $a = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ และ $b = p_1^{f_1} p_2^{f_2} \cdots p_t^{f_t}$ (ซึ่งตัวเลขชี้กำลังบางตัวอาจเท่ากับศูนย์ก็ได้) แล้ว

$$(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_t^{\min(e_t,f_t)},$$
$$[a,b] = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \cdots p_t^{\max(e_t,f_t)},$$

ตัวอย่าง 1.3 *จงหา* $(360, 1597050)$ *และ* $[360, 1597050]$

3. $(a,b)[a,b] = ab$ สำหรับจำนวนเต็ม a, b ใดๆ

4. ถ้า $g \setminus a$ และ $g \setminus b$ แล้ว $g \setminus ax + by$ ซึ่ง x และ y เป็นจำนวนเต็มใดๆ เราเรียก $ax + by$ ว่า เป็น ผลรวมเชิงเส้น (linear combination) ของ a และ b

5. จำนวนเต็มที่ติดตามกัน (กล่าวคือ ผลต่างคือ 1) ย่อมเฉพาะสัมพัทธ์เสมอ

6. ถ้ามีจำนวนเต็ม x, y ซึ่ง $ax + by = 1$ แล้ว $a \perp b$

1.2.1 ทบทวนขั้นตอนวิธีหาร

ในการทบทวนขั้นตอนวิธีหาร เราจะแนะนำหลักการสุดโต่ง (extreme principle) ดังต่อไปนี้

> ถ้าเป็นไปได้ ให้สมมุติว่า สมาชิกของปัญหาเรานั้น มี "ลำดับ" กล่าวคือ สามารถเรียงจากน้อยไปหามาก ดังนั้น หลักการสุดโต่งคือการเพ่งความสนใจของเราไปที่สมาชิก "น้อยที่สุด" และ "ใหญ่ที่สุด" เนื่องจากสองสมาชิกนี้ อาจมีเงื่อนไขบังคับที่น่าสนใจ

ถ้าเรากำลังพิจารณาเซทจำนวนเต็มบวกแล้ว เราจะมีหลักการการเรียงลำดับสมบูรณ์ (Well Ordering Principle) ซึ่งกล่าวว่า

> เซทใดๆ ที่ไม่ว่าง และประกอบด้วยจำนวนเต็มบวก ย่อมมีสมาชิกที่น้อยที่สุด

ตัวอย่าง 1.4 *จงหาสมาชิกที่น้อยที่สุดของเซทต่อไปนี้* $3, 5, 7, 9, \ldots$

ทฤษฎีบท 1.2 *(ขั้นตอนวิธีการหาร) (Division algorithm) ให้* a *และ* b *เป็นจำนวนเต็มบวกโดยที่* $b \geq a$ *แล้ว ย่อมจะมีจำนวนเต็ม* q, r *ซึ่ง* $q \geq 1$ *และ* $0 \leq r \leq a$ *โดยที่*

$$b = qa + r$$

พิสูจน์ โดยการพิจารณาค่าที่ไม่ใช่ลบที่น้อยที่สุดของ $b - at$ โดยที่ t เป็นจำนวนเต็มใดๆ

ดังนั้น เราจะได้ว่า

ตัวหารร่วมมากของ a และ b เป็น ผลรวมเชิงเส้นที่ น้อยที่สุด ของ a และ b

ปัญหา 1.1 *จงแสดงว่า เศษส่วน* $(n^3 + 2n)/(n^4 + 3n^2 + 1)$ *ย่อมลดรูปไม่ได้อีกแล้ว สำหรับทุกจำนวนบวก* n

ปัญหา 1.2 *จงใช้ขั้นตอนวิธีการของยูคลิดหา* $(333, 51)$ *และ* $(89, 24)$

ปัญหา 1.3 สมการดิโอฟันทีน เชิงเส้น *เนื่องจาก* $17 \perp 11$ *ก็ย่อมมีจำนวนเต็ม* x, y *ซึ่ง* $17x + 11y = 1$ *อาทิ* $x = 2, y = -3$ *เราจะสร้างผลเฉลยจำนวนเต็มของ* $17x + 11y = 1$ *เพิ่มเติม โดยเพียงให้*

$$x = 2 + 11tt, y = -3 - 17t,$$

ซึ่ง t *เป็นจำนวนเต็มใดๆ*

1. จงแสดงว่า $x = 2 + 11t, y = -3 - 17t$ ย่อมจะเป็นผลเฉลยของ $17x + 11y = 1$ ไม่ว่า t จะเป็นจำนวนใด

2. จงแสดงว่า ทุกผลเฉลยของ $17x + 11y = 1$ ที่เป็นจำนวนเต็มย่อมอยู่ในรูปนี้

3. จงหา x, y ซึ่ง $89x + 24y = 1$

4. ถ้า $x = 2, y = -3$ **เป็นผลเฉลยของ** $17x + 11y = 1$ **แล้ว** $x = 2u, y = -3u$ **เป็นผลเฉลยของ** $17x + 11y = u$.

5. **ถ้าเราต้องการแก้ปัญหา** $ax + by = c$ **ซึ่ง** a, b, c **เป็นตัวคงที่ เราควรจะทำอย่างไร**

ปัญหา 1.4 *จงแสดงว่า*

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$$

ไม่มีวันเป็นจำนวนเต็มได้

ปัญหา 1.5 *จงแสดงว่า* $1000!$ ***นั้นสิ้นสุดลงด้วย ตัวเลขศูนย์ 249 ตัว*** **จงหาหลักการที่ทั่วไป**

ปัญหา 1.6 *จงแสดงว่า มีจำนวนเฉพาะจำนวนอนันต์ในรูป* $4k+3$

ปัญหา 1.7 *จงแสดงว่า มีจำนวนเฉพาะจำนวนอนันต์ที่มีรูป* $6n-1$

ปัญหา 1.8 *ข้อความต่อไปนี้ จริงหรือเท็จ และเพราะเหตุใด*

1. ผลคูณของจำนวนบวกสองจำนวนที่ติดตามกันไม่อาจเป็นกำลังสองสมบูรณ์ได้

2. ผลคูณของจำนวนบวกสามจำนวนที่ติดตามกันไม่อาจเป็นกำลังสองสมบูรณ์ได้

ปัญหา 1.9 *เมื่อนาย ก ขึ้นเช็คมูลค่า x บาท y สตางค์ เขาได้รับ y บาท x สตางค์ และพบว่า เขามีเงินมากกว่าจำนวนที่ถูกต้อง ตั้ง 2 สตางค์ อยากทราบว่า เช็คนั้น มีมูลค่าเท่าใด*

ปัญหา 1.10 *นาย ฮ. ไปตักน้ำที่ลำธาร โดยมีภาชนะ 9 ลิตร และ 16 ลิตร ตามลำดับ นาย ฮ. จะต้องทำอย่างไร ถึงจะได้น้ำ 1 ลิตรในภาชนะ 16 ลิตร*

2 เลขคณิตมอดุลาร์

ความเป็นเลขคู่ หรือ คี่ ของจำนวนเต็มหนึ่งๆ บอกเราถึง ฐานะของตัวเลขนั้นๆ เมื่อมองจากแง่ของหมายเลข 2 กล่าวคือ ถ้า $2 \setminus n$ ก็หมายความว่า k เป็นเลขคู่ แต่ถ้า 2 หาร k เหลือเศษ 1 แล้ว ก็หมายความว่า k เป็นเลขคี่

ดังนั้น ถ้าเราพิจารณาจำนวนเต็ม $n \geq 2$ แล้ว เราก็ย่อมแบ่งเซทจำนวนเต็มเป็น ชั้นสมภาคต่างๆ ตามเศษที่เหลือหลังจากหารด้วย n แล้ว โดยที่ จำนวนเต็มสองจำนวน จะอยู่ในชั้นสมภาคเดียวกัน ถ้าหารด้วย n แล้ว มีเศษเท่ากัน

ตัวอย่าง 2.1 *พิจารณา* $n = 4$

.

นิยาม 2.1 *จำนวนเต็ม* x *และ* y *ย่อมมีความสัมพันธ์* สมภาคมอดุโล n *กล่าวคือ*

$$x \equiv y(modn)$$

ถ้าทั้งสองมีเศษเท่ากัน เมื่อหารด้วย n

นอกจากนี้ เราอาจมองว่า $x \equiv y$ mod n **ก็ต่อเมื่อ** $n \setminus (x - y)$ **หรือ** $x - y$ **เป็นพหุคูณของ** n
นอกจากนี้ เรามีคุณสมบัติเบื้องต้นของสมภาคมอดุโล n **กล่าวคือ**

1. $x \equiv x$ mod n

2. $x \equiv y$ mod n **มีผลให้** $y \equiv x$ mod n

3. $x \equiv y$ mod n **และ** $y \equiv x$ mod n **มีผลให้** $x \equiv z$ mod n

ดังนั้น สมภาค หรือ คอนกรูเอนซ์ จึงมีคุณสมบัติเหมือนการเท่ากัน นอกจากนี้ เราจะพบว่า มีจำนวนเต็มที่แตกต่างกันเพียง n ตัวเท่านั้น เนื่องจากในการหารด้วย n นั้น จะมีเศษเท่ากับ $0, 1, 2, \ldots, n-1$ เท่านั้น เราเรียกจำนวนเต็มเหล่านี้ว่า จำนวนเต็มมอดุโล n หรือ Z_n

ตัวอย่าง 2.2 *ใน* Z_6 *จงหา* $5+5, 3+13, 2^5$

.

เราจะใช้คำว่า ส่วนตกค้าง มอดุโล n (residue modulo n) อาทิ 7 และ 3 เป็นส่วนตกค้างที่ต่างกัน มอดุโล 5 แต่เป็นส่วนตกค้างที่เท่ากัน มอดุโล 4

ทฤษฎีบท 2.1 *ข้อความ* $a \equiv b$ ***mod*** n *สมมูลกับการที่มีจำนวนเต็ม* k *ซึ่ง* $a = b + nk$

.

ทฤษฎีบท 2.2 *ถ้า* $a \equiv b$ ***mod*** n *และ* $c \equiv d$ ***mod*** n *แล้ว* $a + c \equiv b + d$ ***mod*** n *และ* $ac \equiv bd$ ***mod*** n

ตัวอย่าง 2.3 *จงหาเศษจากการหาร* 2^{1000} *ด้วย* 17

ตัวอย่าง 2.4 *1. ถ้าเขียนจำนวน* n *ในฐาน* 10 *แล้ว* n *ย่อมสมภาคกับผลบวกเลขโดดของมัน มอดุโล* 9 *และ มอดุโล* 3

2. ถ้าเขียนจำนวน n *ในฐาน* 10 *แล้ว* n *ย่อมสมภาคมอดุโล* 11 *กับ เลขโดดหน่วย - เลขโดดหลักสิบ + เลขโดดหลักร้อย - เลขโดดหลักพัน ฯลฯ*

ดังนั้นยุทธศาสตร์หนึ่งก็คือ การมองปัญหา เป็นปัญหามอดุโล n สำหรับตัว n ที่เหมาะสม เพราะมันลดปัญหาที่เกี่ยวข้องกับจำนวนเต็มนับอนันต์มาสู่โลกแห่งจำนวนเต็มเพียง n ตัวเท่านั้น

ตัวอย่าง 2.5 *ถ้า* 127 *คนเล่นในการแข่งขันกีฬาเทนนิส จงแสดงว่า จำนวนคนเป็นจำนวนคู่ ที่เล่นจำนวนเกมเป็นจำนวนคี่*

.

ปัญหา 2.1 *ให้* $N = 22 \cdot 31 + 11 \cdot 17 + 13 \cdot 19$

1. จงหาภาวะคู่หรือคี่ของ N

2. จงหาเลขโดดหน่วยของ N

3. จงหาเศษที่เหลือเมื่อ N ถูกหารด้วย 7

ปัญหา 2.2 *จงหาเลขโดดสองหลักสุดท้ายของ* 3^{1234}

ปัญหา 2.3 จงแสดงว่า *มีพหุคูณบวกของ* 21 *ซึ่งมี* 241 *เป็นตัวเลขสามหลักสุดท้าย*

ปัญหา 2.4 จงแสดงว่า *เมื่อมีเซทของจำนวนเต็ม* n *จำนวนใดๆ จะมีเซทย่อยซึ่งมีผลบวกหารด้วย* n *ลงตัว*

ปัญหา 2.5 *ให้* n *เป็นจำนวนเต็มคี่ซึ่ง* 3 *หารไม่ลงตัว จงแสดงว่า* $n^2 \equiv 1 \ mod\ 24$.

3 สมภาคเชิงเส้นในหนึ่งตัวแปร

นิยาม 3.1 *ให้* a *และ* b *เป็นจำนวนเต็ม เราเรียกสมภาคที่มีรูป* $ax \equiv b$ $\textbf{mod}$ m *ว่า* สมภาคเชิงเส้นในตัวแปร x

ตัวอย่าง 3.1 $2x \equiv 3$ $\textbf{\textit{mod}}$ 4 ***มีผลเฉลยหรือไม่***

.

ตัวอย่าง 3.2 $2x \equiv 3$ $\textbf{\textit{mod}}$ 5 ***มีผลเฉลยหรือไม่***

.

ตัวอย่าง 3.3 $2x \equiv 4$ $\textbf{\textit{mod}}$ 6 ***มีผลเฉลยหรือไม่***

ตัวอย่าง 3.4 *$3x \equiv 9$ mod 6 มีผลเฉลยหรือไม่*

จากตัวอย่างข้างบน เราจึงสนใจ ผลเฉลยอสมภาคโมดุโล m ในเซทจำนวนเต็ม มากกว่าผลเฉลยทั้งหมด เราอาจจะหาผลเฉลยดังกล่าวได้ ด้วยการพิจารณาทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.1 *ให้ $ax \equiv b$ $\mathbf{mod}$ m เป็นสมภาคเชิงเส้น ใน หนึ่งตัวแปร และให้ $d = (a, m)$ ถ้า d หาร b ไม่ลงตัวแล้ว สมภาคนี้ย่อมไม่มีผลเฉลยที่เป็นจำนวนเต็ม แต่ถ้า $d \setminus b$ แล้ว สมภาคนี้ ย่อมมีจำนวน d ผลเฉลยอสมภาคโมดุโล m ที่เป็นจำนวนเต็ม*

อนุนัย 1 *ถ้า $ax \equiv b$ $\mathbf{mod}$ m เป็นสมภาคเชิงเส้นในหนึ่งตัวแปรและให้ $d = (a, m)$ ถ้า $d \setminus b$ แล้ว ทั้ง d ผลเฉลยอสมภาคโมดุโล m ของสมภาคนี้จะหาได้โดย*

$$x_0 + \left(\frac{m}{d}\right) n$$

โดยที่ $n = 0, 1, 2, \ldots, d - 1$, ซึ่ง x_0 จะเป็นผลเฉลยเฉพาะใดๆของสมภาคนี้

ตัวอย่าง 3.5 *จงหาทุกผลเฉลยอสมภาคของสมภาค $16x \equiv 8$ $\mathbf{mod}$ 28*

หนังสืออ้างอิง

[1] R. P. Burn, *A Pathway into Number Theory*, 2nd ed., Cambridge, Cambridge University Press, 1997.

[2] Robert D. Carmichael, *The Theory of Numbers*, New York, John Wiley and Sons, Inc., 1914.

[3] Ronald L. Graham, Donald E. Knuth and Oren Patashnik, *Concrete Mathematics*, New York, Addison-Wesley, 1989.

[4] Loren C. Larson, *Problem-Solving Through Problems*, New York, Springer-Verlag, 1983.

[5] Hans Rademacher and Otto Toeplitz, *The Enjoyment of Math*, Princeton, Princeton University Press, 1994.

[6] Kenneth H. Rosen, *Elementary Number Theory and its applications*, 4th ed., New York, Addison-Wesley, 2000.

[7] James K. Strayer, *Elementary Number Theory*, Boston, PWS Publishing Co., 1994.

[8] Paul Zeitz, *The Art and Craft of Problem Solving*, New York, John Wiley & Sons, Inc., 1999.