



สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี
กระทรวงศึกษาธิการ

ทฤษฎีจำนวน





สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี
กระทรวงศึกษาธิการ

เอกสารเสริมความรู้ วิชาคณิตศาสตร์

ทฤษฎีจำนวน

จัดทำขึ้นเมื่อ ๒๕๖๓

จัดพิมพ์และจัดจำหน่ายโดย



**CHULA
BOOK**

ศูนย์หนังสือจุฬาลงกรณ์มหาวิทยาลัย
www.Chulabook.com

ชื่อเรื่อง	เอกสารเสริมความรู้ วิชาคณิตศาสตร์ เรื่อง ทฤษฎีจำนวน
ชื่อผู้แต่ง	สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) กระทรวงศึกษาธิการ
ลิขสิทธิ์โดย	สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) กระทรวงศึกษาธิการ
พิมพ์ครั้งที่ 2	พ.ศ. 2556
จำนวน	4,000 เล่ม
ราคา	90 บาท

จัดพิมพ์และจัดจำหน่ายโดย



ศูนย์หนังสือจุฬาลงกรณ์มหาวิทยาลัย

อาคารวิทยกิตติ์ ชั้น 14 ซอย จุฬาลงกรณ์ 64 ถนน พญาไท แขวง วังใหม่ เขต ปทุมวัน กรุงเทพฯ 10330

โทรศัพท์ : 0-2255-4433 , 0-2218-9891

Website : <http://www.chulabook.com>



ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี กระทรวงศึกษาธิการ.

เอกสารเสริมความรู้ วิชาคณิตศาสตร์ ทฤษฎีจำนวน.-- กรุงเทพฯ : ไฮแอตพับลิชชิง, 2556.

64 หน้า.

1. ทฤษฎีจำนวนเลข. I. ชื่อเรื่อง.

512.7

ISBN 978-616-237-200-1

พิมพ์ที่ **บริษัท ฐานบัณฑิต จำกัด**

188/5 ซอยเพชรเกษม 51 ถนนเพชรเกษม แขวงบางแคเหนือ เขตภาษีเจริญ กรุงเทพฯ 10160

โทร. 0 2801 3934-8

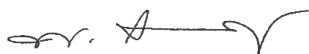
นายสมัย ต่ายสกุลทิพย์ ผู้พิมพ์ผู้โฆษณา

คำนำ

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) เป็นหน่วยงานในกำกับของกระทรวงศึกษาธิการ มีหน้าที่หลักสำคัญประการหนึ่ง คือ การวิจัยและพัฒนาหลักสูตร หนังสือเรียน คู่มือครู ตลอดจนสื่อและเอกสารส่งเสริมการเรียนรู้ กลุ่มสาระการเรียนรู้คณิตศาสตร์ กลุ่มสาระการเรียนรู้วิทยาศาสตร์ รวมทั้งสาระการออกแบบและเทคโนโลยีและสาระเทคโนโลยีสารสนเทศ และการสื่อสารในกลุ่มสาระการเรียนรู้การงานอาชีพและเทคโนโลยี

ภารกิจหลักสำคัญอีกประการหนึ่งของ สสวท. ได้แก่การส่งเสริมศักยภาพของนักเรียนที่มีความสามารถและสนใจทางด้านวิทยาศาสตร์ คณิตศาสตร์และเทคโนโลยี สสวท. จึงได้พัฒนาหนังสือชุดนี้ขึ้นสำหรับผู้ที่มีความสนใจและนักเรียนที่มีความสามารถพิเศษทางคณิตศาสตร์ หนังสือชุดนี้มีด้วยกันทั้งหมด 8 เล่ม คือ พีชคณิต เรขาคณิต สมการเชิงฟังก์ชัน ทฤษฎีจำนวน ตรรกศาสตร์เบื้องต้น และวิธีการพิสูจน์ คอมบินาทอริก อสมการ และทฤษฎีกราฟเบื้องต้น ซึ่งหนังสือชุดนี้จะให้ความรู้ทางคณิตศาสตร์ที่ลึกซึ้งขึ้นจากบทเรียนตามหลักสูตร นักเรียน ครู และผู้ที่สนใจ ที่ต้องการพัฒนาความรู้ความสามารถทางคณิตศาสตร์ให้ดียิ่งขึ้นควรศึกษาหนังสือชุดนี้ และหนังสือชุดนี้ยังเหมาะสมกับนักเรียนชั้นเรียนพิเศษทางด้านวิทยาศาสตร์และคณิตศาสตร์ในระดับมัธยมศึกษาตอนปลาย รวมถึงเป็นพื้นฐานที่ดีแก่ผู้ที่ต้องการเตรียมตัวสมัครเข้ารับการรับการอบรมในค่ายโอลิมปิกวิชาการอีกด้วย

ในการจัดพิมพ์หนังสือชุดนี้ในครั้งนี้ สสวท. ได้ปรับปรุงเนื้อหาให้เหมาะสมยิ่งขึ้น โดยได้รับความร่วมมืออย่างดียิ่งจากคณาจารย์และผู้ทรงคุณวุฒิจากหลายหน่วยงาน สสวท. หวังเป็นอย่างยิ่งว่าหนังสือชุดนี้จะเป็นประโยชน์สำหรับครูและนักเรียน ตลอดจนผู้สนใจ และขอขอบคุณทุกท่านที่ได้มีส่วนร่วมในการจัดทำหนังสือชุดนี้ไว้ ณ โอกาสนี้



(นางพรพรรณ ไวทยางกูร)

ผู้อำนวยการสถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี
กระทรวงศึกษาธิการ

คำนำ

ในการพิมพ์ครั้งที่ 1

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) ได้รับมอบหมายจากกระทรวงศึกษาธิการให้พัฒนาหลักสูตร หนังสือเรียน คู่มือครู ตลอดจนสื่อประกอบการเรียนการสอน วิชาคณิตศาสตร์วิทยาศาสตร์และเทคโนโลยี เพื่อช่วยส่งเสริมให้การเรียนการสอนวิชาคณิตศาสตร์วิทยาศาสตร์และเทคโนโลยี บรรลุผลสำเร็จตามวัตถุประสงค์ของหลักสูตร

เอกสารเสริมความรู้เล่มนี้จัดทำขึ้นเพื่อเผยแพร่ความรู้ทางคณิตศาสตร์ในระดับมัธยมศึกษา และระดับอุดมศึกษาให้กับนักเรียน นักศึกษา อาจารย์และผู้สนใจ สำหรับศึกษาค้นคว้าในอันที่จะพัฒนาความรู้ ความสามารถทางคณิตศาสตร์ให้ดียิ่งขึ้น

สสวท. หวังเป็นอย่างยิ่งว่าเอกสารเล่มนี้จะเป็นประโยชน์สำหรับผู้อ่าน และขอขอบคุณทุกท่านที่ได้มีส่วนร่วมในการจัดทำเอกสารเล่มนี้ไว้ ณ โอกาสนี้



(นายพิศาล สร้อยสุหร่ำ)

ผู้อำนวยการสถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี
กระทรวงศึกษาธิการ

คำชี้แจง

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) ได้พัฒนาหนังสือชุดนี้ เพื่อเสริมความรู้วิชาคณิตศาสตร์ให้กับนักเรียนที่มีความสามารถพิเศษทางคณิตศาสตร์ได้เพิ่มเติมศักยภาพของตัวเองให้สูงสุด และสำหรับครูคณิตศาสตร์ที่จะต้องสอนนักเรียนห้องเรียนที่มีความสามารถพิเศษทางคณิตศาสตร์ด้วยเนื้อหาและลำดับขั้นตอนการนำเสนอในหนังสือชุดนี้ได้อิงความรู้ที่นักเรียนได้เรียนมาแล้วตามหลักสูตร ถ้าหากหัวข้อเรื่องใดที่อิงความรู้พื้นฐานที่นักเรียนยังไม่ได้เรียน หนังสือชุดนี้ได้สรุปเนื้อหาพื้นฐานนั้นไว้ก่อนเพื่อเชื่อมโยงให้นักเรียนสามารถศึกษาได้อย่างเป็นลำดับขั้นของความรู้ เพื่อให้ผู้สนใจสามารถค้นคว้าและศึกษาได้ด้วยตนเอง

หนังสือชุดนี้มี 8 เล่ม นักเรียนหรือคุณครูจะเลือกเรียนหรือเลือกสอนเรื่องใดก่อนก็ได้ ด้วยมีเนื้อหาเป็นอิสระแก่กัน คณะกรรมการจัดทำได้พยายามอย่างยิ่งที่จะพัฒนาหนังสือชุดนี้ให้เป็นหนังสือที่สมบูรณ์ อย่างไรก็ตาม หากท่านพบข้อบกพร่องหรือมีข้อเสนอแนะเพิ่มเติม โปรดส่งข้อเสนอแนะของท่านไปยังสาขาคณิตศาสตร์มัธยมศึกษา สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี จะเป็นพระคุณอย่างยิ่ง ทั้งนี้ เพื่อเป็นประโยชน์ในการปรับปรุงเอกสารให้สมบูรณ์มากยิ่งขึ้น

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี
กระทรวงศึกษาธิการ

สารบัญ

บทนำ

ก

บทที่ 1 การหารลงตัว

1

บทที่ 2 จำนวนเฉพาะ

17

บทที่ 3 คอนกรูเอนซ์

32

บทที่ 4 ผลเฉลยของคอนกรูเอนซ์กำลังหนึ่ง

41

บทที่ 5 ทฤษฎีบทเศษเหลือของจีน

46

บทที่ 6 จำนวนในฐานต่าง ๆ

57

บทนำ

ทฤษฎีจำนวนเป็นวิชาที่ศึกษาเกี่ยวกับจำนวนเต็ม คือ $0, 1, -1, 2, -2, \dots$ เนื่องจากจำนวนเต็ม เป็นจำนวนจริง ดังนั้น จึงสอดคล้องกับสมบัติต่าง ๆ ของจำนวนจริง เซตของจำนวนเต็มซึ่งเป็นสับเซตของเซตของจำนวนจริง มีสมบัติปิดและมีเอกลักษณ์ภายใต้การบวกและการคูณ และจำนวนเต็มทุกตัว มีอินเวอร์สภายใต้การบวก แต่อินเวอร์สภายใต้การคูณของจำนวนเต็มที่ไม่เป็นศูนย์ อาจไม่เป็นจำนวนเต็ม ซึ่งทำให้ได้ว่า สำหรับจำนวนเต็ม a, b ที่ $b \neq 0$ เศษส่วน $\frac{a}{b}$ อาจจะเป็นจำนวนเต็มหรือไม่เป็นจำนวนเต็มก็ได้ เช่น $\frac{4}{2} = 2$ เป็นจำนวนเต็ม แต่ $\frac{3}{2}$ ไม่เป็นจำนวนเต็ม ในกรณีที่ $\frac{a}{b}$ เป็นจำนวนเต็ม เรากล่าวว่า จำนวนเต็ม b หารจำนวนเต็ม a ลงตัว และ b เป็นตัวหารของ a เราจะพิจารณาสมบัติต่าง ๆ ของจำนวนเต็มที่เกี่ยวข้องกับตัวหาร

เราจะแทนเซตของจำนวนตรรกยะ หรือเศษส่วนของจำนวนเต็มทั้งหมดด้วย $\mathbb{Q}$ เซตของจำนวนเต็มทั้งหมดด้วย $\mathbb{Z}$ และเซตของจำนวนเต็มบวกทั้งหมดด้วย $\mathbb{Z}^+$ หรือ $\mathbb{N}$

เซตของจำนวนเต็มบวกมีสมบัติที่สำคัญซึ่งเราจะใช้อยู่เสมอคือ

หลักอุปนัยเชิงคณิตศาสตร์ (Principle of Mathematical Induction)

ให้ n_0 เป็นจำนวนเต็ม และสำหรับทุก ๆ จำนวนเต็ม $n \geq n_0$

ให้ $p(n)$ เป็นข้อความเกี่ยวกับ n ซึ่ง

(ก) $p(n_0)$ จริง

และ (ข) ทุก ๆ $k \geq n_0$, ถ้า $p(k)$ จริง แล้ว $p(k+1)$ จริง

แล้วจะสรุปได้ว่า ทุก ๆ จำนวนเต็ม $n \geq n_0$, $p(n)$ จริง

หลักอุปนัยเชิงคณิตศาสตร์อย่างเข้ม (Principle of Strong Mathematical Induction)

ให้ n_0 เป็นจำนวนเต็ม และสำหรับทุก ๆ จำนวนเต็ม $n \geq n_0$

ให้ $p(n)$ เป็นข้อความเกี่ยวกับ n ซึ่ง

(ก) $p(n_0)$ จริง

และ (ข) ทุก ๆ $k \geq n_0$, ถ้า $p(n_0), p(n_0 + 1), \dots, p(k)$ จริง แล้ว $p(k + 1)$ จริง แล้ว

จะสรุปได้ว่า ทุก ๆ จำนวนเต็ม $n \geq n_0$, $p(n)$ จริง

หลักการจัดอันดับดี (Well - Ordering Principle)

สำหรับ $S \subset \mathbb{N}$ ใด ๆ ถ้า $S \neq \emptyset$ แล้ว S มีสมาชิกค่าน้อยสุด

ให้ x เป็นจำนวนจริงใด ๆ จะมีจำนวนเต็ม c ค่ามากที่สุดที่ $c \leq x$
ทำให้ได้ว่า $x < c + 1$ เราแทนจำนวนเต็ม c ดังกล่าวด้วย $\lfloor x \rfloor$ และเรียกว่า
ภาคจำนวนเต็มของ x

ให้ $\varepsilon = x - c$ จะได้ว่า $0 \leq \varepsilon < 1$ และเรียก ε ว่า ภาคเศษของ x
นั่นคือ แต่ละจำนวนจริง x จะสามารถเขียนอยู่ในรูป $x = c + \varepsilon$ โดยที่ c เป็น
จำนวนเต็ม และ ε เป็นจำนวนจริงที่ $0 \leq \varepsilon < 1$
(หมายเหตุ การกำหนด $\lfloor x \rfloor$ ดังกล่าว เป็นฟังก์ชันจากเซตของจำนวนจริงไปยัง
เซตของจำนวนเต็มและเรียกว่า ฟังก์ชันจำนวนเต็มมากที่สุด)

ต่อไปให้ a และ b เป็นจำนวนเต็มใด ๆ โดยที่ $b \neq 0$ จะได้ว่า จำนวนเศษส่วน $\frac{a}{b}$
จะเขียนอยู่ในรูป

$$\frac{a}{b} = c + \varepsilon$$

โดยที่ c เป็นจำนวนเต็ม และ $0 \leq \varepsilon < 1$

บทนิยาม 1.1 ให้ a และ b เป็นจำนวนเต็ม โดยที่ $b \neq 0$ เราจะกล่าวว่า b หาร a ลงตัว ซึ่งแทนด้วย $b|a$ ก็ต่อเมื่อ $\frac{a}{b}$ เป็นจำนวนเต็ม ในกรณีนี้ เราเรียก b ว่า เป็นตัวหารของ a และเรียก a ว่าเป็นพหุคูณของ b

ถ้า b หาร a ไม่ลงตัว จะแทนด้วย $b \nmid a$

ตัวอย่าง 1.1 $3|6$ แต่ $3 \nmid -5$

หมายเหตุ จากนิยามของ $b|a$ เรากำหนดให้ $b \neq 0$ ดังนั้น เมื่อเขียนสัญลักษณ์ $b|a$ ให้เป็นที่เข้าใจว่า ตัวหาร $b \neq 0$

ทฤษฎีบท 1.1 ให้ a, b, c เป็นจำนวนเต็มใดๆ จะได้ว่า

$$\text{ก) } a|b \wedge b \neq 0 \rightarrow |a| \leq |b|$$

$$\text{ข) } a|b \wedge b|a \rightarrow a = \pm b$$

$$\text{ค) } a|b \wedge a|c \rightarrow a|(bx + cy) \quad \text{ทุก ๆ จำนวนเต็ม } x \text{ และ } y$$

พิสูจน์ ก) สมมติให้ $a|b$ และ $b \neq 0$

ดังนั้น จะมีจำนวนเต็ม c ที่ทำให้ $b = ac$ จาก $b \neq 0$ ทำให้ $c \neq 0$ ดังนั้น $|c| \geq 1$ และ $|b| = |ac| = |a||c| \geq |a|$

ข) สมมติให้ $a|b$ และ $b|a$ ดังนั้น $a \neq 0$ และ $b \neq 0$

จาก (ก) จะได้ว่า $|a| \leq |b|$ และ $|b| \leq |a|$ นั่นคือ $|a| = |b|$ ทำให้ $a = \pm b$

ค) เว้นไว้เป็นแบบฝึกหัด

ข้อสังเกต จากทฤษฎีบท 1.1 (ค) แทนค่า $c=0$ จะได้ว่า

$$a|b \rightarrow a|bx \quad \text{สำหรับทุก ๆ จำนวนเต็ม } x$$

ทฤษฎีบท 1.2 (ขั้นตอนวิธีการหาร)

สำหรับจำนวนเต็ม a และ b ใดๆ ที่ $b > 0$ จะมีจำนวนเต็ม q และ r เพียงคู่เดียวที่ทำให้

$$a = bq + r \quad \text{โดยที่ } 0 \leq r < b$$

พิสูจน์ ให้ a และ b เป็นจำนวนเต็มที่ $b > 0$

ดังนั้น $\frac{a}{b} = q + \varepsilon$ เมื่อ q เป็นจำนวนเต็ม และ $0 \leq \varepsilon < 1$

จึงได้ว่า $a = bq + b\varepsilon$ ทำให้ $b\varepsilon = a - bq$ เป็นจำนวนเต็มให้เป็น r

เนื่องจาก $b > 0$ และ $0 \leq \varepsilon < 1$ จะได้ว่า $0 \leq r = b\varepsilon < b$

นั่นคือ มีจำนวนเต็ม q และ r ที่ทำให้ $a = bq + r$ โดยที่ $0 \leq r < b$

ต่อไปจะพิสูจน์ว่า มีคู่เดียวที่มีสมบัติว่า มี q', r' ที่ทำให้ $a = bq' + r'$

โดยที่ $0 \leq r' < b$ ให้ $bq + r = bq' + r'$ และ $-b < -r' \leq 0$

$$0 - b < r - r' < b + 0$$

ทำให้ $-1 = \frac{-b}{b} < \frac{r - r'}{b} = q' - q < \frac{b}{b} = 1$ และ $q' - q$ เป็นจำนวนเต็ม

ดังนั้น $q' - q = 0 = r - r'$ นั่นคือ $q = q'$ และ $r = r'$

ตัวอย่าง 1.2

ก) $a = 478, b = 7$

เนื่องจาก $478 = 7 \cdot 68 + 2$ ดังนั้น $q = 68, r = 2$

ข) $a = -478, b = 7$

เนื่องจาก $-478 = 7(-69) + 5$ ดังนั้น $q = -69, r = 5$

ข้อสังเกต เมื่อหารจำนวนเต็ม a ใดๆ ด้วย 2 จะได้ว่า เศษเหลือ r เป็น 0 หรือ 1

ถ้า $r = 0$ จะได้ว่า $a = 2c + 0 = 2c$

และถ้า $r = 1$ จะได้ว่า $a = 2c + 1$

ดังนั้น จำนวนเต็มทุกตัวจะอยู่ในรูป $2c$ หรือ $2c + 1$ ใดๆอย่างหนึ่งเพียงอย่างเดียว

บทนิยาม 1.2

จำนวนเต็ม a เป็นจำนวนคู่ ก็ต่อเมื่อ มีจำนวนเต็ม c ที่ $a = 2c$

a เป็นจำนวนคี่ ก็ต่อเมื่อ มีจำนวนเต็ม c ที่ $a = 2c + 1$

จากบทนิยาม จะได้ว่า a เป็นจำนวนเต็มคู่ ก็ต่อเมื่อ $2 \mid a$

ตัวอย่าง 1.3

จงพิสูจน์ว่า สำหรับจำนวนเต็ม a ใดๆ $2 \mid a(a + 1)$

ผลคูณของจำนวนเต็มที่เรียงกันสองจำนวนเป็นจำนวนคู่เสมอ

(นั่นคือ $\forall a \in \mathbb{Z}, a(a + 1)$ เป็นจำนวนคู่เสมอ)

พิสูจน์ ให้ a เป็นจำนวนเต็มใดๆ

กรณี 1 a เป็นจำนวนคู่ นั่นคือ $2 \mid a$ ดังนั้น จะได้ว่า $2 \mid a(a + 1)$

กรณี 2 a เป็นจำนวนคี่ ดังนั้น จะมีจำนวนเต็ม c ที่ $a = 2c + 1$

$$\text{ทำให้ } a + 1 = 2c + 2 = 2(c + 1)$$

$$\text{นั่นคือ } 2 \mid (a + 1) \quad \text{จึงได้ว่า } 2 \mid a(a + 1)$$

ตัวอย่าง 1.3 จะเป็นกรณีพิเศษของตัวอย่างต่อไปนี

ตัวอย่าง 1.4 จงพิสูจน์ว่า สำหรับจำนวนเต็มบวก n ใด ๆ ผลคูณของจำนวนเต็มที่เรียงกัน n ตัวใด ๆ จะหารลงตัวด้วย n เสมอ

พิสูจน์ ให้ n เป็นจำนวนเต็มบวกใด ๆ และให้ a เป็นจำนวนเต็มใด ๆ

เราจะพิสูจน์ว่า ผลคูณ $a(a + 1)(a + 2) \dots (a + n - 1)$ จะหารลงตัวด้วย n

โดยขั้นตอนวิธีการหาร จะมีจำนวนเต็ม q และ r ที่ทำให้ $a = nq + r$ โดยที่ $0 \leq r < n$

กรณี 1 $r = 0$ จะได้ว่า $n \mid a$ ทำให้ได้ว่า $n \mid a(a + 1) \dots (a + n - 1)$

กรณี 2 $1 \leq r < n$ จะได้ว่า $1 \leq n - r \leq n - 1$ ทำให้ได้ว่า $a + 1 \leq a + n - r \leq a + n - 1$

$$\text{และ } a + n - r = nq + r + n - r = n(q + 1)$$

$$\text{ดังนั้น } n \mid (a + n - r) \text{ ซึ่งทำให้ } n \mid a(a + 1) \dots (a + n - r) \dots (a + n - 1)$$

เนื่องจากทุก ๆ จำนวนเต็ม $x \neq 0$, $x \mid 0$ ดังนั้น 0 จะมีตัวหารอยู่เป็นจำนวนอนันต์ และสำหรับจำนวนเต็ม $a \neq 0$ ถ้า x เป็นตัวหารของ a จะได้ว่า $|x| \leq |a|$ โดยทฤษฎีบท 1.1 (ก) นั่นคือ a จะมีตัวหารอยู่เป็นจำนวนจำกัด

ต่อไปให้ a และ b เป็นจำนวนเต็ม และพิจารณาตัวหารของทั้ง a และ b ซึ่งเรียกว่าตัวหารร่วมของ a และ b ถ้า $a = 0$ และ $b = 0$ จะได้ว่า จำนวนเต็มที่ไม่เป็น 0 ทุกตัวจะเป็นตัวหารร่วม ซึ่งทำให้ไม่น่าสนใจแต่สำหรับกรณีที่ $a \neq 0$ หรือ $b \neq 0$ จะได้ว่า ตัวหารร่วมของ a และ b มีจำนวนจำกัด และเนื่องจาก d เป็นตัวหารร่วมของ a และ b ก็ต่อเมื่อ $-d$ จะเป็นตัวหารร่วมของ a และ b ดังนั้น เราจึงพิจารณาเฉพาะตัวหารร่วมที่เป็นบวก นอกจากนี้ ถ้า d เป็นตัวหารร่วมของ a และ b และ $d' \mid d$ จะได้ว่า d' จะเป็นตัวหารร่วมของ a และ b ด้วย ดังนั้น ถ้าเราทราบตัวหารร่วมค่ามากที่สุด เราจะได้ตัวหารร่วมทั้งหมดของ a และ b

บทนิยาม 1.3 ให้ a และ b เป็นจำนวนเต็มที่ $a \neq 0$ หรือ $b \neq 0$ และ d เป็นจำนวนเต็มบวก d เป็น ตัวหารร่วมของ a และ b ก็ต่อเมื่อ $d \mid a$ และ $d \mid b$ และ d เป็นตัวหารร่วมมากที่สุดของ a และ b แทนด้วย $d = (a, b)$ ก็ต่อเมื่อ