

รายงานการวิจัย

เรื่อง ตัวหารของฟังก์ชันเลขคณิต (Divisors of arithmetic functions)

ชื่อผู้วิจัย นายวิเชียร เลาท โกศล
นางสาวกรรณิกา คงสาคร
นางสาวอุษณีย์ ธีรวัฒน์

ได้รับทุนอุดหนุนการวิจัยจากสำนักงานคณะกรรมการวิจัยแห่งชาติ ประเภท ทั่วไป
ประจำปี 2534

ปีที่พิมพ์ 2538

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

บทคัดย่อ

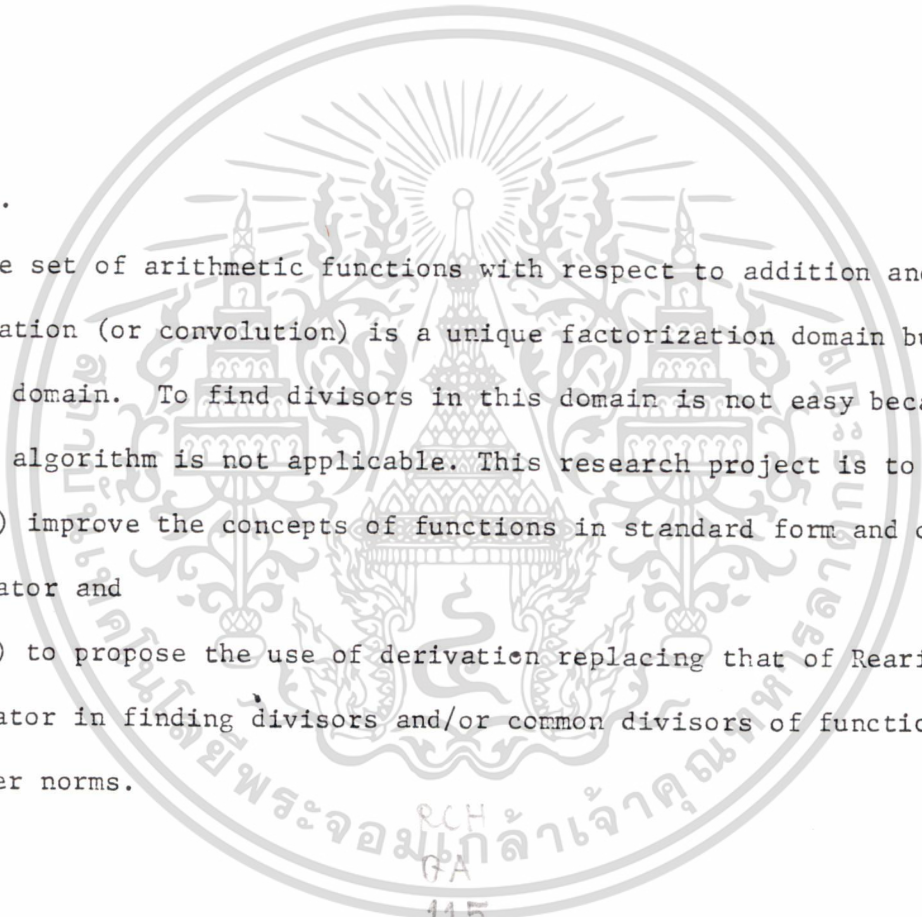
เซตของฟังก์ชัน เลขคณิต เมื่อเทียบกับการบวกและการคูณดิริค เลต (หรือการประสาน) ประกอบกัน เป็นโดเมนที่แยกตัวประกอบได้หนึ่งเดียว แต่ไม่เป็นโดเมนยุคลิด การหาตัวหารในโดเมนนี้เป็นสิ่งไม่ง่าย เพราะ ขั้นตอนวิธีของยุคลิดไม่สามารถนำมาใช้ได้ โครงการวิจัยนี้มีผลสรุปดังนี้

- (1) ปรับปรุงแนวคิดของฟังก์ชันที่อยู่ในรูปมาตรฐาน และตัวดำเนินการคล้ายอนุพันธ์ ให้ชัดเจนและเหมาะสม
- (2) สร้างเทคนิคใหม่โดยใช้การหาอนุพันธ์ทดแทนวิธีการเดิมของ เรียร์ริกที่ใช้ตัวดำเนินการคล้ายอนุพันธ์ ในการหาตัวหาร และ/หรือตัวหารร่วมมากของฟังก์ชันที่มีค่าประจำ เป็นกำลังของจำนวนเฉพาะ

Abstract.

The set of arithmetic functions with respect to addition and Dirichlet multiplication (or convolution) is a unique factorization domain but not an Euclidean domain. To find divisors in this domain is not easy because the Euclidean algorithm is not applicable. This research project is to

- (1) improve the concepts of functions in standard form and derivative-like operator and
- (2) to propose the use of derivation replacing that of Rearick's derivative-like operator in finding divisors and/or common divisors of functions with prime power norms.



ECH
GA
115
956101

เลขหมู่.....
 เลขทะเบียน **117608**
 รับเดือนปี 1.0 ส.ค. 2554

b. 12345678
 i.....

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญเรื่อง

บทนำ	1
เนื้อเรื่อง	4
-รูปมาตรฐานและอนุพันธ์ของฟังก์ชัน เลขคณิต	5
-Divisors of some arithmetic functions	8
บรรณานุกรม	
ประวัตินักวิจัยและคณะ	



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทนำ

ความสำคัญ และที่มาของหัวข้อการวิจัย

ฟังก์ชัน เลขคณิต (Arithmetic functions) คือฟังก์ชันค่าเชิงซ้อนที่มีโดเมนเป็นเซตของจำนวนเต็มบวก ผลบวก ผลต่าง ผลคูณ (สามัญ) ผลคูณดิริคเลต (Dirichlet) หรือผลคูณเลขคณิต หรือผลการประสาน (convolution) ของฟังก์ชัน เลขคณิต f และ g มีนิยามเป็นฟังก์ชัน เลขคณิต ที่มีคุณสมบัติต่อไปนี้

$$(f \pm g)(n) := f(n) \pm g(n)$$

$$(fg)(n) := f(n) g(n)$$

$$(f * g)(n) := \sum_{ij=n} f(i) g(j)$$

เมื่อ k เป็นจำนวนเต็มบวก นิยาม

$$f^{*k} := f * f * \dots * f \quad (k \text{ ครั้ง})$$

เมื่อ c เป็นจำนวนเชิงซ้อน นิยามฟังก์ชัน เลขคณิต cf โดย

$$(cf)(n) := cf(n)$$

ให้ A เป็นเซตของฟังก์ชัน เลขคณิต เป็นที่ทราบกันว่า $[1, 4]$ A เป็นโดเมนเชิงจำนวนเต็ม (integral domain) เทียบกับการบวก และการประสาน โดเมน A มีตัวแทนอื่นอีก 2 แบบ คือ เป็นโดเมนของอนุกรมกำลังนัยนิยม (formal power series) ในตัวไม่กำหนดจำนวนนับได้ และเป็นโดเมนของอนุกรมดิริคเลตนัยนิยม [4]

นิยามฟังก์ชันเอกลักษณ์ u โดย

$$u(n) = \begin{cases} 1 & \text{ถ้า } n = 1 \\ n & \text{อื่น ๆ} \end{cases}$$

เซตของฟังก์ชัน เลขคณิต cu (เมื่อ c แปรไปเหนือจำนวนเชิงซ้อน) ประกอบกันเป็นวงย่อยของ A ที่ถอดแบบ (isomorphic) กับสนามเชิงซ้อน \mathbb{C} ฟังก์ชัน u เป็นเอกลักษณ์เทียบกับการประสานใน A ดังนั้น ตัวผกผันดิริคเลต f^{-1} ของ f เป็นฟังก์ชัน เลขคณิตหนึ่งเดียว (unique) ที่ว่า $f * f^{-1} = u$ เราสามารถตรวจสอบได้โดยง่ายว่า f^{-1} มีจริง เมื่อและต่อเมื่อ $f(1) \neq 0$ [1]

โครงการวิจัยที่เสนอนี้มีที่มาจากความจริงที่ว่า แม้น A จะไม่เป็นโดเมนกลุ่มอุดมคติมูลฐานสำคัญ (principal ideal domain) ดังนั้นจึงไม่เป็นโดเมนยูคลิด (Euclidean domain) แต่มันเป็นโดเมนที่มีการแยกตัวประกอบหนึ่งเดียว (unique factorization domain) [4] ที่ว่า A ไม่ใช่โดเมนกลุ่ม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

อุดมคติมุขสำคัญ สามารถเห็นจริงได้โดยใช้แนวคิดของค่าประจำ (norm) ค่าประจำ Nf ของฟังก์ชัน

เลขคณิต f มีนิยามเป็นจำนวนเต็มบวกค่าต่ำสุด n ที่ว่า $f(n) \neq 0$ เห็นได้ชัดเจนว่า

$N(f * g) = Nf \cdot Ng$ และตัวหนึ่งหน่วย (units) ของ A คือฟังก์ชันเลขคณิตที่มีค่าประจำเป็น 1 เนื่องจาก

เซตของฟังก์ชันที่ไม่ใช่ตัวหนึ่งหน่วยใน A ประกอบกันเป็นกลุ่มอุดมคติที่ไม่เป็นมุขสำคัญ ดังนั้น A เป็นโดเมน

กลุ่มอุดมคติมุขสำคัญไม่ได้ [2,5,12] ส่วนความจริงที่ว่า A เป็นโดเมนที่มีการแยกตัวประกอบหนึ่งเดียว

พิสูจน์ได้ไม่ย่ายนัก ในหลักการแล้ว การพิสูจน์ทำผ่านตัวแทนของ A ที่เป็นโดเมนของอนุกรมกำลังนัยนิยมใน

ตัวไม่กำหนดจำนวนนับได้ ขั้นตอนสำคัญในการพิสูจน์ คือใช้ผลที่ว่า การแยกตัวประกอบหนึ่งเดียว เป็นจริงใน

วงของทุกอนุกรมกำลังใน n ตัวไม่กำหนด สำหรับค่า $n = 1, 2, 3, \dots$ ([2,5,12])

โดยเหตุที่เป็นโดเมนที่มีการแยกตัวประกอบหนึ่งเดียวซึ่งมีลักษณะ เฉพาะติดปรกติ เช่นนี้ ปัญหาแรก

ที่สำคัญ คือ การหาขั้นตอนและผลที่เกี่ยวข้องกับตัวหาร (divisors) โดยเฉพาะอย่างยิ่ง ตัวหารร่วมมาก

จากลักษณะเฉพาะของมัน เราเห็นว่า ขั้นตอนวิธีของยุคลิด (Euclidean algorithm) ที่ใช้กันโดยทั่วไป

ใช้ไม่ได้โดยตรงในกรณีนี้ ทำให้ต้องแสวงหาขั้นตอนวิธีแบบใหม่ เท่าที่ทราบจนถึงปัจจุบันนี้ มีเพียงงานวิจัยที่

พิมพ์เผยแพร่เพียงชิ้นเดียว เกี่ยวกับขั้นตอนวิธีใหม่ดังกล่าว ซึ่งคืองานของ D. Rearick (1984)

นอกจากแนวคิดของค่าประจำ แล้ว เรียริค ใช้แนวคิดอื่น ๆ อีกหลายแนวคิด ดังต่อไปนี้

ให้ f เป็นฟังก์ชันเลขคณิตที่มีค่าประจำ a เรียริคแสดงว่า มีตัวหนึ่งหน่วย v ใน A เพียงตัวเดียว

ที่ว่า

$$S_f(na) := (v * f)(na) = u(n)$$

สำหรับแต่ละจำนวนเต็มบวก n S_f มีชื่อเรียกว่ารูปมาตรฐาน (standard form) ของ f

และเรากล่าวว่า f อยู่ในรูปมาตรฐาน เมื่อและต่อเมื่อ $f = S_f$

ให้ p เป็นจำนวนเฉพาะ นิยาม

$$r(n) := \begin{cases} 1 & \text{เมื่อ } n = p \\ 0 & \text{อื่น ๆ} \end{cases}$$

นิยามการส่ง $f \rightarrow f'$ ของ A ไปใน A โดย $f'(n) := f(np)$

โดยใช้แนวคิดของโครงสร้างนี้ เรียริค พัฒนาระเบียบวิธีในการหาสูตรสำหรับตัวหารร่วมมากในรูป

มาตรฐานที่มีค่าประจำสูงสุดใน A สิ่งที่ได้เป็นแคลคูลัสเชิงอนุพันธ์ที่น่าไปสู่การประยุกต์ใช้สร้างสมการพหุนาม

ที่มีตัวหารร่วมมากของฟังก์ชันเลขคณิตคู่หนึ่ง ๆ เป็นราก ข้อบกพร่องข้อหนึ่งของงานของเรียริค คือข้อจำกัดที่ว่า

ฟังก์ชันเลขคณิตที่ใช้ระเบียบวิธีนี้ได้จะต้องมีค่าประจำเป็นกำลังของจำนวนเฉพาะจำนวนเดียวกัน

ก่อนหน้าผู้วิจัยได้ดำเนินการตรวจสอบงานของเรียริค พบว่าการใช้ตัวดำเนินการคล้ายอนุพันธ์ f'

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า และ ร คอนข้างไม่สะดวก และ แลดูผิดธรรมชาติ น่าจะเป็นการเหมาะสมกว่าที่จะใช้แนวคิดของอนุพันธ์ p -มูลฐาน ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

(p-basic derivation) ([13]) ซึ่งนิยามโดย

$$df(n) := f(np)v(np)$$

เมื่อ $v(m)$ เป็นกำลังสูงสุดของ p ที่หาร m ลงตัว

หัวใจหลักของโครงการวิจัยนี้ เพื่อสร้างระเบียบวิธีในการหาตัวหารในวงของฟังก์ชัน เลขคณิตที่ดีกว่าของ เรียร์ค ตลอดจนดัดแปลงแก้ไขวิธีการของ เรียร์ค ให้ทันสมัย ชัดเจน รัดกุม

วัตถุประสงค์ของโครงการวิจัย

- (1) เพื่อปรับปรุงผลงานของ เรียร์ค เกี่ยวกับฟังก์ชันในรูปมาตรฐาน และตัวดำเนินการคล้ายอนุพันธ์
- (2) เพื่อสร้างระเบียบวิธี และ/หรือ เทคนิคใหม่โดยใช้การหาอนุพันธ์

ขอบเขตการวิจัย

- (1) ฟังก์ชันที่พิจารณาคือ ฟังก์ชัน เลขคณิต
- (2) ปฏิบัติการของฟังก์ชัน เลขคณิตที่พิจารณา คือ การบวก และการประสาน
- (3) ตัวหารของฟังก์ชัน เลขคณิต คือตัวหาร เทียบกับการประสาน
- (4) วิธีการที่ใช้คือการอนุพันธ์ และค่าอนุวัต

วิธีดำเนินการวิจัย

- (1) สืบรวจ เอกสาร ข้อมูล และผลงานที่เกี่ยวข้องทั้งในและนอกประเทศ
- (2) ปรับปรุงผลงานของ เรียร์ค โดยวิธีการทำให้ฟังก์ชันในรูปมาตรฐาน ชัดเจน รัดกุม
- (3) สร้างระเบียบวิธี และ/หรือ เทคนิคใหม่ในการหาตัวหารโดยใช้แนวคิดของการหาอนุพันธ์
- (4) ติดต่อ สอบถาม แลก เปลี่ยน สิ่งที่ค้นพบกับผู้ทรงคุณวุฒิทั้งในและนอกประเทศ
- (5) รวบรวมผล และพิมพ์เผยแพร่

ประโยชน์ที่คาดว่าจะได้รับ

- (1) ได้ปรับปรุงฟังก์ชันในรูปมาตรฐานให้ชัดเจน รัดกุม ทำให้ผลของ เรียร์ค เป็นที่ยอมรับ ยืนยัน อีกครั้งหนึ่ง
- (2) ได้ระเบียบวิธี และ/หรือ เทคนิคโดยใช้การหาอนุพันธ์ทดแทนวิธีการเดิมที่ใช้ตัวดำเนินการคล้ายอนุพันธ์ในการหาตัวหาร

เนื้อเรื่อง

รายละเอียดเกี่ยวกับวิธีดำเนินการวิจัย และผลการวิจัย ในโครงการวิจัยนี้ ได้เสร็จเรียบร้อย และนำเสนอในวารสาร และการประชุมทางวิชาการ

1. เรื่อง รูปมาตรฐานและอนุพันธ์ของฟังก์ชัน เลขคณิต

ปรากฏใน ว. เกษตรศาสตร์(วิทย์.) 26:307-309 (2535)

2. เรื่อง Divisors of some arithmetic functions

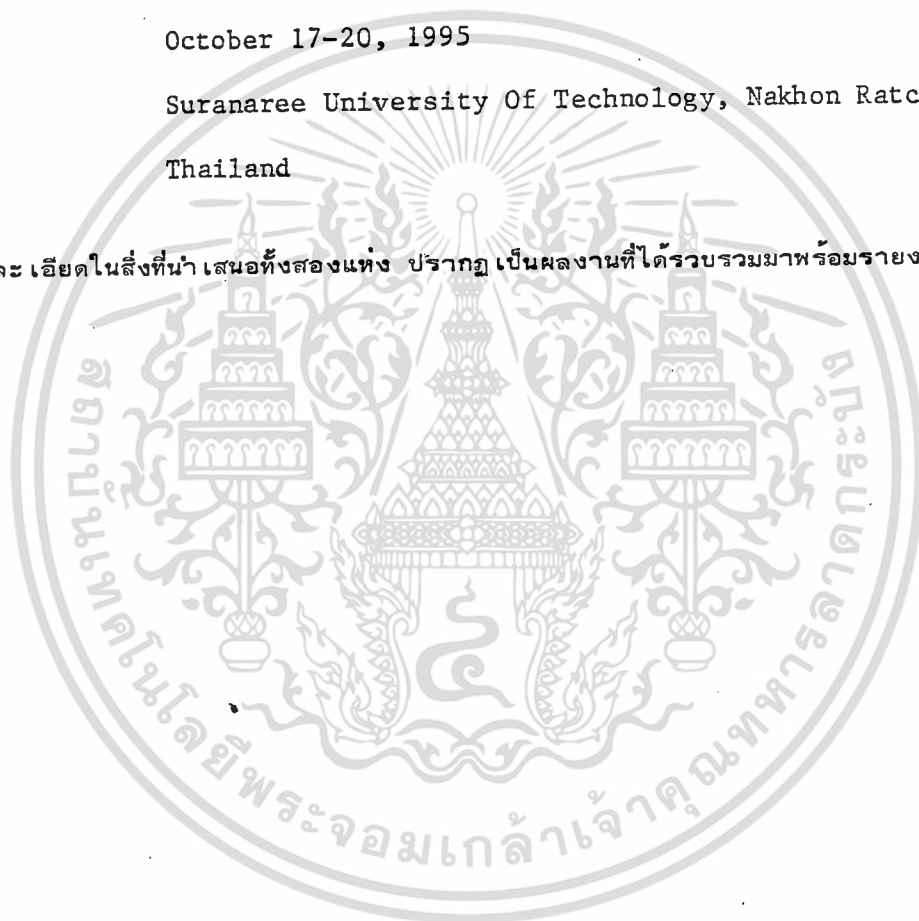
นำเสนอในการประชุม The Second Asian Mathematical Conference

October 17-20, 1995

Suranaree University Of Technology, Nakhon Ratchasima,
Thailand

รายละเอียดในสิ่งที่น่าสนใจทั้งสองแห่ง ปรากฏ เป็นผลงานที่ได้รับรวบรวมมาพร้อมรายงานฉบับนี้

ในหน้าถัดไป



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปมาตรฐานและอนุพันธ์ของฟังก์ชันเลขคณิต

Standard Forms and Derivatives of Arithmetic Functions

วิเชียร เลหาโกศล และ กรรณิกา คงสาคร¹
Vichian Laohakosol and Kannika Kongsakorn

ABSTRACT

The set of arithmetic functions with respect to addition and Dirichlet multiplication is a unique factorization domain but not an Euclidean domain... To find divisors in this domain is not easy. The concepts of functions in standard form and derivative-like operator due to Rearick are neither clear nor appropriate. A modification of these concepts are carried out.

Key words : arithmetic function, Dirichlet multiplication, divisors, standard form, derivative.

บทคัดย่อ

เซตของฟังก์ชันเลขคณิตเมื่อเทียบกับการบวกและการคูณดิริคเลต ประกอบกันเป็นโดเมนที่แยกตัวประกอบได้หนึ่งเดียวแต่ไม่เป็นโดเมนยูคลิด การหาตัวหารในโดเมนนี้เป็นสิ่งไม่ง่าย แนวคิดของฟังก์ชันที่อยู่ในรูปมาตรฐานและตัวดำเนินการคล้ายอนุพันธ์ซึ่งเป็นของเรียริคไม่ชัดเจนและไม่เหมาะสม งานนี้เป็นการปรับปรุงแนวคิดทั้งสองให้รัดกุมและชัดเจน เหมาะสม

คำนำ

ฟังก์ชันเลขคณิตพร้อมด้วยปฏิบัติการบวก (+) และการคูณดิริคเลต (*) ประกอบกันเป็นโดเมนเชิงจำนวนเต็ม A ที่มีตัวแทนได้อีกสองแบบ คือ โดเมนของอนุกรมกำลัง นัยนิยมในตัวไม่กำหนดจำนวนนับได้ และโดเมนของอนุกรมดิริคเลต นัยนิยม เมื่อปี พ.ศ. 2531 ผู้วิจัยได้

เสนองานวิจัยว่าด้วยความเป็นอิสระต่อกันเชิงเลขคณิต โดยการพิสูจน์ความเป็นอิสระของฟังก์ชันเลขคณิตจำนวนหนึ่ง (กรรณิกา และคณะ 2531; Laohakosol et al., 1989 a,b) นอกจากความเป็นอิสระเชิงพีชคณิตแล้ว ปัญหาพื้นฐานอีกปัญหาหนึ่งที่เกี่ยวข้องกับโครงสร้างของ A คือ ปัญหาว่าด้วยการแยกตัวประกอบของสมาชิกใน A เนื่องจาก A เป็นโดเมนที่แยกตัวประกอบได้หนึ่งเดียว แต่ไม่เป็นโดเมนยูคลิด (Buchsbaum, 1961; Cashwell and Everett, 1959; Krull, 1937; Ruckert, 1933; Samuel, 1961) การแยกตัวประกอบหรือการหาตัวหารของสมาชิกใน A จึงเป็นสิ่งยากมาก เท่าที่ทราบจนถึงปัจจุบันนี้ มีงานวิจัยเผยแพร่เพียงงานของ Rearick (1984) ซึ่งแสดงการหาตัวหารเพียงของสมาชิกบางประเภท จากการศึกษางานดังกล่าว พบปัญหาสำคัญ 2 ข้อคือ ปัญหาข้อที่ 1 มีความไม่ชัดเจนในนิยามว่าด้วยฟังก์ชันอยู่ในรูปมาตรฐาน และ ปัญหาข้อที่ 2 ว่าด้วยความไม่เหมาะสมในการใช้ตัวดำเนินการคล้ายอนุพันธ์ ทั้งสองปัญหาขยายความได้ดังนี้

¹ ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

Department of Mathematics, Faculty of Science, Kasetsart University, Bangkok 10900, Thailand.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ให้ f เป็นฟังก์ชันเลขคณิตที่ไม่ใช่ศูนย์ นิยามค่าประจำของ f (เขียนแทนด้วย Nf) เป็นจำนวนเต็มบวก a ค่าต่ำสุด ที่ว่า $f(a) \neq 0$ Rearick เรียกฟังก์ชัน f ว่าอยู่ในรูปมาตรฐาน เมื่อ

$$f(an) = u(n) \quad (n = 1, 2, 3, \dots)$$

โดยที่ $u(n) = 1$ เมื่อ $n = 1$ และ $u(n) = 0$ เมื่อ n มีค่าอื่น ๆ กล่าวคือเป็นฟังก์ชันเอกลักษณ์เทียบกับการคูณตรีคเลต นิยามนี้ไม่ชัดเจน เพราะขาดความเป็นหนึ่งเดียว กล่าวคือฟังก์ชันที่อยู่ในรูปมาตรฐานเดียวกัน (เช่นมีค่าประจำเท่ากัน) มีเป็นจำนวนมาก และไม่ทราบอีกด้วยว่าสำหรับฟังก์ชันที่ไม่ทราบว่าจะอยู่ในรูปมาตรฐานหรือไม่ สามารถนำแนวคิดนี้มาใช้ได้อย่างไร

ในกรณีของตัวดำเนินการคล้ายอนุพันธ์ Rearick นิยามสิ่งนี้เป็น

$$f'(n) = f(np) \quad (n = 1, 2, 3, \dots)$$

เมื่อ p เป็นจำนวนเฉพาะที่ตรงไว้ค่าหนึ่ง ความไม่เหมาะสมของตัวดำเนินการนี้ คือสูตรการหาอนุพันธ์ของการคูณล้มเหลว กล่าวคือ $(f * g)' \neq f' * g + f * g'$

วัตถุประสงค์ของงานวิจัยนี้คือ ขจัดความไม่ชัดเจนของนิยามฟังก์ชันที่อยู่ในรูปมาตรฐาน และปรับปรุงตัวดำเนินการคล้ายอนุพันธ์ให้เป็นตัวดำเนินการอนุพันธ์

อุปกรณ์และวิธีการ

อุปกรณ์และวิธีการหลักที่ใช้ประกอบด้วย

ก. นิยามและคุณสมบัติพื้นฐานของฟังก์ชันเลขคณิต ซึ่งในการวิจัยครั้งนี้ยึดสิ่งที่ใช้ใน กรรณิกา และคณะ (2531) Laohakosol et al. (1989 a,b) เป็นหลัก

ข. วิธีการหาอนุพันธ์อีติววิธีการของ Shapiro (1972) โดยพิจารณาตัวดำเนินการอนุพันธ์- p (เมื่อ p เป็นจำนวนเฉพาะที่ตรงจำนวนหนึ่ง) ของฟังก์ชันเลขคณิตที่ไม่เป็นศูนย์ f ให้เป็น

$$df(n) = f(np)v(np)$$

เมื่อ $v(n)$ เป็นกำลังสูงสุดของ p ที่หาร n ลงตัว โปรดสังเกตว่า df มีคุณสมบัติของตัวดำเนินการอนุพันธ์ทุกประการ

ค. ทฤษฎีบทประกอบต่อไปนี้ของ Rearick (1984)

ทฤษฎีบทประกอบ ให้ $f \in A - \{0\}$, $Nf = a$ ดังนั้นมีฟังก์ชันหนึ่งหน่วย (ฟังก์ชันที่มีค่าประจำเป็น 1) w_f เพียงฟังก์ชันเดียวพอดี ที่มีคุณสมบัติว่า $(w_f * f)(na) = u(n)$ ($n = 1, 2, 3, \dots$)

ผลและวิจารณ์

การจัดความไม่ชัดเจนของฟังก์ชันที่อยู่ในรูปมาตรฐานดังในปัญหาข้อที่ 1 ทำได้โดยใช้ผลจากทฤษฎีบทประกอบ สร้างนิยามต่อไปนี้

นิยาม (1) ให้ $f \in A - \{0\}$, $Nf = a$ นิยามรูปมาตรฐานของ f เป็นฟังก์ชัน $S_f = w_f * f$ เมื่อ w_f เป็นฟังก์ชันหนึ่งเดียว (เมื่อเทียบกับ f) ที่ยืนยันการมีอยู่จริงได้จากทฤษฎีบทประกอบ

(2) นิยามว่าฟังก์ชัน f อยู่ในรูปมาตรฐาน ถ้า $f(na) = u(n)$

ข้อดีของนิยามข้างต้นต่อของ Rearick คือ (1) ชัดเจนเพราะแต่ละฟังก์ชันมีรูปมาตรฐานได้หนึ่งเดียว ส่วนความถูกต้องชัดเจนของ (2) นั้น เป็นผลมาจากทฤษฎีบทต่อไปนี้ ทฤษฎีบท ให้ $h \in A - \{0\}$ ดังนั้น h อยู่ในรูปมาตรฐานเมื่อและต่อเมื่อ $h = S_h$

พิสูจน์ (ความเพียงพอของเงื่อนไข) ให้ $h = S_h$ ดังนั้นโดยนิยาม (1), (2) และทฤษฎีบทประกอบ จะได้ว่า h อยู่ในรูปมาตรฐานทันที

(ความจำเป็นของเงื่อนไข) ให้ $Nh = b$ เพราะว่า h เป็นฟังก์ชันเลขคณิตที่ไม่เป็นศูนย์ ดังนั้น โดยทฤษฎีบทประกอบ จะมีฟังก์ชันหนึ่งหน่วย w_h เพียงหนึ่งเดียวที่ว่า

$$S_h(nb) = (w_h * h)(nb) = u(n) \quad (n = 1, 2, 3, \dots)$$

การพิสูจน์จะเสร็จสิ้นถ้าสามารถแสดงได้ว่า $w_h = u$ (เอกลักษณ์ของการคูณตรีคเลต) เมื่อ $n = 1$

$$1 = u(1) = (w_h * h)(1.b) = w_h(1)h(b) = w_h(1).1 = w_h(1)$$

เมื่อ $n \geq 2$ เรามีว่า

$$\begin{aligned} 0 &= u(n) = (w_h * h)(nb) = \sum_{d|nb} w_h(d)h(nb/d) \\ &= w_h(n)h(b) = w_h(n). \end{aligned}$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ดังนั้น $w_n = u$ ตามต้องการ

ในส่วนของกรณปัญหาที่ 2 ทำโดยการใช้ตัวดำเนินการอนุพันธ์ $-p$ df ดังที่ได้กล่าวถึงในหัวข้อ "อุปกรณ์และวิธีการ" แทนตัวดำเนินการคล้ายอนุพันธ์ f' ความเหมาะสมในการใช้ df นอกจากการคงไว้ซึ่งกฎการหาอนุพันธ์ของผลคูณที่ว่า

$$d(f \cdot g) = df \cdot g + f \cdot dg$$

แล้ว เพื่อเป็นการยืนยันความเหมาะสม จึงควรจะต้องว่าคุณสมบัติที่เรียกได้ว่าเป็นการหาอินทิกรัลของ f เทียบกับตัวดำเนินการคล้ายอนุพันธ์ สามารถแสดงให้เห็นจริงได้โดยง่ายจากการใช้ df ดังต่อไปนี้

$$\text{ให้ } r(n) = \begin{cases} 1 & \text{เมื่อ } n = p \\ 0 & \text{เมื่อ } n \neq p \end{cases}$$

ดังนั้น $(r \cdot f)' = f$ กล่าวคือ อินทิกรัลของ f เทียบกับ $'$ คือ $r \cdot f$

พิสูจน์ ก่อนอื่นขอให้สังเกตว่า

$$df(n) = f(np)v(np) = f(n)v(np)$$

$$dr(n) = r(np)v(np) = \begin{cases} 1 & \text{เมื่อ } n = 1 \\ 0 & \text{เมื่อ } n \neq 1 \end{cases}$$

$$v(np) = v(n) + v(p) = v(n) + 1$$

พิจารณา

$$\begin{aligned} (r \cdot f)'(n) \cdot v(np) &= d(r \cdot f)(n) = dr \cdot f(n) + r \cdot df(n) \\ &= dr(1)f(n) + \begin{cases} r(p)df(n/p) & \text{เมื่อ } pln \\ 0 & \text{เมื่อ } pln \end{cases} \\ &= f(n) + \begin{cases} f(n)v(n) & \text{เมื่อ } pln \\ 0 & \text{เมื่อ } pln \end{cases} \end{aligned}$$

เพราะฉะนั้น เมื่อ pln ได้ว่า $(r \cdot f)'(n) (v(n)+1) = f(n) (1+v(n))$

$$\text{ซึ่งให้ว่า } (r \cdot f)'(n) = f(n)$$

และเมื่อ $p+n$ ได้ว่า $(r \cdot f)'(n) (0+1) = f(n)$

$$\text{ซึ่งให้เช่นกันว่า } (r \cdot f)'(n) = f(n)$$

คำขอขอบคุณ

งานวิจัยนี้เป็นส่วนหนึ่งของโครงการวิจัยเรื่อง ตัวหาร

ของฟังก์ชันเลขคณิต ซึ่งได้รับทุนอุดหนุนการวิจัยประเภททั่วไป ประจำปีงบประมาณ 2534 จากสำนักงานคณะกรรมการวิจัยแห่งชาติ

เอกสารอ้างอิง

กรณิกา คงสาคร วิเชียร เลาทโกศล และอุษณีย์ สิริวัฒน์.

2531. ความเป็นอิสระต่อกันของฟังก์ชันเลขคณิต. ว.เกษตรศาสตร์ (วิทย์.). 22(3) : 213-220.

Buchsbaum, D.A. 1961. Some remarks on factorization in power series rings. J. Math. Mech. 10(5) : 749-753.

Cashwell, E.D. and C.J. Everett. 1959. The ring of number-theoretic functions. Pacific J. Math. 9 : 975- 985.

Krull, W. 1937. Beitrage zur Arithmetik Kommutativer Integritatsbereiche. III Zum Dimensionsbegriff der Idealtheorie. Math. Z. 42 : 745-766.

Laohakosol, V. K. Kongsakorn and U. Leerawat. 1989 a. Some arithmetic functions algebraically independent with respect to convolution. Soochow J. Math. 15(2) : 171-178.

Laohakosol, V., K. Kongsakorn and U. Leerawat. 1989b. Algebraic independence test of arithmetic functions using Jacobians. J. Sci. Soc. Thailand. 15 : 133-138.

Rearick, D. 1984. Divisibility of arithmetic functions. Pacific J. Math. 112(1) : 237-248.

Ruckert, W. 1933. Zum Eliminationsproblem der Potenzreihenideale. Math. Ann.. 107 : 259-281.

Samuel, P. 1961. On unique factorization domains. III. J. Math. 5 : 1-17.

Shapiro, H.N. 1972. On the convolution ring of arithmetic functions. Comm. Pure Appl. Math. 25 : 287-336.



DIVISORS OF SOME ARITHMETIC FUNCTIONS

VICHIAN LAOHAKOSOL
Department of Mathematics
Kasetsart University
Bangkok 10900, Thailand

It is well-known that the set of arithmetic functions equipped with addition and Dirichlet multiplication (or convolution) is a unique factorization domain but not a Euclidean domain. With the powerful Euclidean algorithm not being directly applicable, it is not easy to find divisors of two arithmetic functions in this domain. The existing technique of using a derivative-like operator due to D. Rearick is rather awkward. A slightly different technique based on the use of a derivation is proposed and generally proceeds along similar line.

1. Introduction

An *arithmetic function* is a complex-valued function whose domain is the set of positive integers, \mathbb{N} . The sum, difference, (ordinary) product and Dirichlet product (or *convolution*) of two arithmetic functions are arithmetic functions defined, respectively, by

$$(f \pm g)(n) = f(n) \pm g(n)$$

$$(fg)(n) = f(n)g(n)$$

$$(f * g)(n) = \sum_{ij=n} f(i)g(j).$$

For brevity, when k is a positive integer, write f^k for $f * f * \dots * f$ (k times). For each complex number c , the arithmetic function cf is defined by

$$(cf)(n) = cf(n).$$

Denote by Λ the set of all arithmetic functions. It is well-known that Λ is an integral domain with respect to addition and convolution ([1],[2]). The domain Λ has two other representations, one as the domain of (formal) Dirichlet series and the other as the domain of (formal) power series in a countable set of indeterminates ([2],[5]). Define the *identity function* by

$$I(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

117608

Clearly, the set of arithmetic functions cI , where c runs through the complex numbers, forms a subring of Λ isomorphic to the complex field. The function I plays the role of the identity with respect to convolution and so the (Dirichlet) inverse f^{-1} of f is the (unique) arithmetic function for which $f * f^{-1} = I$. It is easily verified that f^{-1} is in Λ if and only if $f(1) \neq 0$ ([1]).

Our interests germinate from the fact that even though Λ is not a principal ideal domain, and so not an Euclidean domain, it is a unique factorization domain ([2]). That Λ is not a principal ideal domain can be seen by making use of the concept of "norm". For each f in $\Lambda - \{0\}$, define its *norm*, Nf , to be the smallest positive integer n such that $f(n) \neq 0$. The norm has a multiplicative property, i.e. $N(f * g) = Nf \cdot Ng$, and the *units* of Λ are those arithmetic functions whose norms are equal to 1. Since the set of non-units in Λ forms an ideal which is not principal, then Λ cannot be a principal ideal domain. That Λ is a unique factorization domain is difficult to prove. Indeed, this was established through the representation of formal power series in a countable set of indeterminates. A major step of the proof is to appeal to the fact that unique factorization holds in the ring of all formal power series in n indeterminates for each positive integer n . Being a unique factorization domain of quite an unusual character, one natural question is to ask for procedures and results about divisors, in particular, greatest common divisors. Evidently, the familiar Euclidean algorithm is not directly applicable, and we have to resort to different means. There has been only one published work known to us, that of D. Rearick ([4]). Besides the concept of norm, Rearick used certain other notions, which we now elaborate.

For an arithmetic function f with $Nf = s$, Rearick showed that there exists a unique unit function u_f such that

$$S_f(ns) := (u_f * f)(ns) = I(n) \quad (n \in \mathbb{N}).$$

The function $S_f := u_f * f$ is called the *standard form* of f , and f is said to be *in standard form* if and only if $f(ns) = I(n)$. For a prime number p , define the (derivative-like) function $f' (= f'_p)$ by $f'(n) = f(np)$. Based upon such a setting, Rearick developed a method of obtaining formulae for certain common divisors. There are several awkwardnesses in Rearick's presentation, e.g. (i) a slight ambiguity in the meaning of functions in standard form, that we quickly clarify in our first lemma, (ii) the use of a derivative-like operator f' is rather unnatural as witnessed via the failure of identities like $(f * g)' \neq f' * g + g' * f$. We propose here to employ the p -basic derivation ([6], [7]), which is a truly legitimate derivation. Further, the concept of norm, convenient in the entire discussion, could also be related and replaced by the valuation $|f| := 1/(Nf)$, which is a truly legitimate nonarchimedean valuation.

2. Standard Form and Derivation

We record for completeness a lemma of Rearick alluded to in Section 1, which will be frequently quoted. The proof of this lemma is straight-forward.

REARICK'S LEMMA. *Let f be in Λ with norm $Nf = s$. Then there exists a unique unit function u_f in Λ such that $S_f := u_f * f$ is in standard form.*

Our next lemma confirms the uniqueness of the standard form.

LEMMA 1. *Let f be in $\Lambda - \{0\}$, and let S_f be its standard form. Then f is in standard form if and only if $f = S_f$.*

PROOF. if $f = S_f$, then the fact that f is in standard form follows immediately from the definition of S_f . Now assume that f is in standard form, i.e.

$$f(ns) = I(n) \quad (n \in \mathbb{N}, s = Nf)$$

From the definition of S_f , there exists a unique unit function u_f such that $S_f = u_f * f$. It remains to show that $u_f = I$, which follows readily from

$$1 = I(1) = S_f(s) = (u_f * f)(s) = u_f(1),$$

and for $n \geq 2$,

$$0 = I(n) = S_f(ns) = (u_f * f)(ns) = u_f(n).$$

□

Next, we recall the definition of derivation and establish certain preliminary results.

DEFINITION ([5]). A *derivation* d over Λ is a mapping of Λ into itself satisfying $d(f * g) = df * g + f * dg$, $d(c_1f + c_2g) = c_1df + c_2dg$, where f, g are in Λ , and c_1, c_2 are complex numbers. Two typical examples of derivation are

(i) the *p -basic derivation*, p prime, defined by

$$(d_p f)(n) = f(np)v(np) \quad (n \in \mathbb{N}),$$

where $v(m)(= v_p(m))$ denotes the exponent of the highest power of p dividing m ,

(ii) the *log-derivation* defined by

$$(d_L f)(n) = f(n) \log n \quad (n \in \mathbb{N}).$$

REMARK. Each derivation annihilates all constant functions, and all usual rules of differentiation hold for a derivation.

LEMMA 2. Let f, e_0, e_1, \dots, e_m be in Λ , with $e_m \neq 0$. Let d be a derivation on Λ . If

$$\sum_{i=0}^m e_i * f^i = 0$$

and $de_i = 0$ ($i = 0, \dots, m$), then $df = 0$.

PROOF. Taking the derivation of the equation, we obtain

$$df * \sum_{i=0}^m e_i * i f^{i-1} = 0.$$

If $df \neq 0$, then $\sum e_i * i f^{i-1} = 0$, and by taking successive derivations, the order of the resulting equations are reduced by 1 each time. Finally, we arrive at $m!e_m = 0$, which is absurd. \square

LEMMA 3. Let p_1, \dots, p_r be distinct primes, and d_1, \dots, d_r be their corresponding p_i -basic derivations. Let f be in Λ , having norm $Nf = p_1^{a_1} \dots p_r^{a_r}$, with a_1, \dots, a_r positive integers. Then f is in standard form if and only if

$$d_1^{a_1} \dots d_r^{a_r} f(n) = a_1! \dots a_r! I(n) \quad (n \in \mathbb{N}).$$

PROOF. The result follows directly from the identity

$$d_1^{k_1} \dots d_r^{k_r} f(n) = f\left(np_1^{k_1} \dots p_r^{k_r}\right) \prod_{i_1=1}^{k_1} v_1(np_1^{i_1}) \dots \prod_{i_r=1}^{k_r} v_r(np_r^{i_r})$$

where $v_i = v_{p_i}$. \square

LEMMA 4. Let $h, f, g \in \Lambda$ be such that

$$\sqrt{h} = f * g, \quad Nf = p^a, \quad Ng = p^b,$$

where p is a prime, and a and b are nonnegative integers. If among h, f, g two are in standard form, then so is the third.

PROOF. Suppose that f and g are in standard form, then by Lemma 3,

$$d^a f(n) = a! I(n), \quad d^b g(n) = b! I(n) \quad (n \in \mathbb{N}),$$

where d is the p -basic derivation. Since $d^i f = 0$ if $i > a$, $d^j g = 0$ if $j > b$, then

$$\begin{aligned} d^{a+b} h(n) &= \sum_{i=0}^{a+b} \binom{a+b}{i} d^i f * d^{a+b-i} g(n) \\ &= \binom{a+b}{a} d^a f * d^b g(n) = (a+b)! I(n), \end{aligned}$$

and so by Lemma 3, h is in standard form with $Nh = p^{a+b}$.

Suppose that g and h are in standard form with $h = f * g$. By Rearick's lemma, there exists a unique unit function u_f such that $u_f * f$ is in standard form. Now

$$u_f * h = (u_f * f) * g$$

and so by the first part of the lemma, the right-hand side being a product of two functions in standard form must be in standard form and so is $u_f * h$. But h is already in standard form and by the uniqueness of u_f , we must have $u_f = I$. \square

REMARK. (i) If h is in standard form where Nh is a power of a prime p and h can be factored as $h = f * g$, let u_f be the unique unit function for which $u_f * f$ is in standard form. Then we can write $h = (u_f * f) * (u_f^{-1} * g)$, which by Lemma 4 implies that $u_f^{-1} * g$ is in standard form. It follows that in the (unique) prime factorization of an arithmetic function in standard form, each prime factor can be taken as in standard form.

(ii) The result of Lemma 4 does not hold if the norms involved are not a power of the same prime.

LEMMA 5. Let p be a prime with p -basic derivation d . If f and g are arithmetic functions in standard form with $Nf = p$, $Ng = p^b$, $b \in \mathbb{N}$, then

$$\sum_{k=0}^{b+1} \frac{(-1)^k}{k!} f^k * d^k(f * g) = 0.$$

PROOF. Put $h = f * g$. Since f is in standard form with norm p , then

$$d^k h = f * d^k g + k d^{k-1} g.$$

Multiplying by f^k , and letting k be $b+1$ and b , we get

$$f^{b+1} * d^{b+1} h = (b+1) f^{b+1} * d^b g.$$

$$f^b * d^b h = f^{b+1} * d^b g + b f^b * d^{b-1} g,$$

and so after subtraction,

$$f^{b+1} * d^{b+1} h - (b+1) f^b * d^b h = -(b+1) b f^b * d^{b-1} g.$$

Continuing in this manner, we have the required result. \square

LEMMA 6. Let $h \in \Lambda$ be in standard form, with $Nh = p^4$, p a fixed prime. Then there is a sixth degree polynomial

$$T(f) := f^6 + A * f^5 + B * f^4 + C * f^3 + B * h * f^2 + A * h^2 * f + h^3,$$

where $A = -\frac{1}{2} d^2 h$, $B = \frac{1}{6} dh * d^3 h - h$, $C = -(dh)^2 - \frac{1}{36} h * (d^3 h)^2 + h * d^2 h$ are differential polynomials in h , of norms p^2, p^4, p^6 , respectively, such that every

divisor f of h of norm p^2 , in standard form, is a root of T . Furthermore, every root of T lying in Λ is a divisor of h , of norm p^2 .

PROOF. Suppose $h = f * g$, with f, g in standard form with $Nf = Ng = p^2$. By taking repeated derivations, we get

$$dh = df * g + f * dg, \quad d^2h = 2!f + 2df * dg + 2!g, \quad d^3f = 3!df + 3!dg.$$

Eliminating df, dg and g among these four equations, we obtain the form $T(f) = 0$ satisfied by f .

Conversely, assume f is a root of T lying in Λ . If $Nf < p^2$, then the term f^6 in $T(f)$ would be the unique term of the smallest norm, so $T(f) \neq 0$. Similarly, we cannot have $Nf > p^2$, and so $Nf = p^2$. Next, we show that $f|h$. By unique factorization, if $f \nmid h$, then there is a prime q in Λ which divides f to a power higher than that to which it divides h , say $q^m | f$, $q^{m-1} | h$ but $q^m \nmid h$. Every term of T is then divisible by q^{3m-2} except for the last, so $T(f) \neq 0$, which is impossible. \square

LEMMA 7. Let h_0, h_1 be in Λ with $Nh_0 = Nh_1 = p^4$, $\Delta d^3h \neq 0$. If f , lying in Λ , is a root of T , with d being p -derivation,

$$V(f) := (\Delta h)^2 - \frac{1}{2} \Delta h * \Delta d^2h * f + \frac{1}{6} \Delta dh * \Delta d^3h * f - \frac{1}{36} (\Delta d^3h)^2 * f^3,$$

then $f | \Delta h$ and $d^2f = 3!I$.

PROOF. If $Nf < p^2$, then the term $-\frac{1}{36} (\Delta d^3h)^2 * f^3$ in $V(f)$ would be the unique term of the smallest norm, so $V(f) \neq 0$. Similarly, we cannot have $Nf > p^2$, so $Nf = p^2$. Again, proceeding as in the proof of the last lemma, we have $f | \Delta h$. Finally, to show that $d^2f = I$, rewrite $\Delta h * V(f) = 0$ as

$$0 = u^3 + \left(-\frac{1}{12} (\Delta d^2h)^2 + \frac{1}{6} \Delta dh * \Delta d^3h\right) * u \\ + \left(-\frac{1}{108} (\Delta d^2h)^3 + \frac{1}{36} \Delta dh * \Delta d^2h * \Delta d^3h - \frac{1}{36} (\Delta d^3h)^2 * \Delta h\right),$$

where $u := \frac{\Delta h}{f} - \frac{1}{3!} \Delta d^2h$. Observe that each coefficient (of u) has zero p -derivation, and so by Lemma 2, we get $d\left(\frac{\Delta h}{f}\right) = -\frac{1}{3!} \Delta d^3h$. Using this last relation, together with taking p -derivation of the equation in u twice, we get $\frac{\Delta h}{f} = \frac{1}{3!} \Delta d^3h$. Substituting this last relation in the equation $\frac{V(f)}{f^3} = 0$, then dividing by Δd^3h , and taking p -derivation, we arrive at $d^2f = 3!I$. \square

3. Results

THEOREM 1. Let $h \in \Lambda$ be in standard form with $Nh = p^c$, where p is a fixed prime and c a nonnegative integer. Consider the following polynomial in f :

$$P(f) := \sum_{k=0}^c \frac{(-1)^k}{k!} f^k * d^k h,$$

where d is the p -basic derivation. Then the roots of p lying in Λ are exactly the divisors of h of norm p , in standard form.

PROOF. If f is a divisor of h with $Nf = p$ and in standard form, then $h = f * g$ with $Ng = p^{c-1}$. By Lemma 4, g is also in standard form, and so by Lemma 5, we have $P(f) = 0$.

On the other hand, assume $P(f) = 0$. Define the arithmetic function

$$r(n) := \begin{cases} 1 & \text{if } n = p, \\ 0 & \text{otherwise,} \end{cases}$$

and note that r is in standard form with $dr = I$. Writing $P(f)$ as a polynomial in $f - r$, we get

$$0 = \sum_{k=0}^c \frac{(-1)^k}{k!} d^k h * (f - r + r)^k = \sum_{i=0}^c \frac{(-1)^i}{i!} C_i * (f - r)^i,$$

where

$$C_i = \sum_{k=0}^{c-i} \frac{(-1)^k}{k!} r^k * d^{k+i} h.$$

Observe that $C_c = d^c h = c!I \neq 0$, and $dC_i = 0$ for all i . Thus, by Lemma 2, $d(f - r) = 0$ and so $df = I$. Since f is a root of $P(f) = 0$, then f divides the constant term of $P(f)$, which is $P(0) = h$. Consequently, $Nf = p^a$, for some nonnegative integer a not greater than c . Hence, f is not a unit and we conclude that $Nf = p$, with f in standard form. \square

CONVENTION. For brevity, throughout the rest of the paper, all functions considered are understood as arithmetic functions, p is a fixed prime, and d is the corresponding p -basic derivation.

THEOREM 2. Let h be in standard form with $Nh = p^2$. Then

(i) h is a square if and only if h satisfies the differential equation

$$(dh)^2 - 4h = 0,$$

(ii) h is a prime if and only if $(dh)^2 - 4h$ is not a square.

PROOF. The result follows by taking the case $c = 2$ in Theorem 1, and observing that the quadratic equation so obtained has discriminant equal to $(dh)^2 - 4h$. \square

THEOREM 3. Let h be in standard form with $Nh = p^c$, c being a positive integer. Consider the following polynomial in f over the field of quotients of Λ :

$$Q(f) := \sum_{k=0}^c \frac{(-1)^k}{k!} d^k h * h^k * f^{c-k}.$$

Then the roots of Q lying in Λ are exactly the divisors of h in standard form with norm p^{c-1} .

PROOF. Observe that $Q(f) = P(h/f) * f^c$, where P is the polynomial stated in Theorem 1. If $h = f * g$, with f in standard form and $Nf = p^{c-1}$, then $g = h/f$ is in standard form of norm p , so that by Theorem 1, $P(g) = 0$, and so $Q(f) = 0$.

Conversely, assume $Q(f) = 0$. Then $P(h/f) = 0$, with h/f belonging to the field of quotients of Λ . Since P is monic, then h/f is in Λ , i.e. $f \mid h$. By Theorem 1, $N(h/f) = p$, so $Nf = p^{c-1}$. Also by Theorem 1, h/f is in standard form, and so f is in standard form. \square

DEFINITION. Let h_0, h_1 be in standard form, both having norm equal to a power of p . By a *differential polynomial* in h_0, h_1 we mean a polynomial in h_0, h_1 and their derivatives with constant coefficients. By a *differential rational form* in h_0, h_1 we mean an arithmetic function expressed as a quotient of two differential polynomials in h_0, h_1 .

THEOREM 4. Let h_0, h_1 be in standard form, not equal, each of norm p^2 . Then h_0 and h_1 have a non-unit common divisor if and only if they satisfy the differential equation

$$(\Delta h)^2 - \Delta h * \Delta dh * dh_i + (\Delta dh)^2 * h_i = 0 \quad (i = 0, 1), \quad (1)$$

where $\Delta h = h_1 - h_0$. Moreover, if (1) holds, this common divisor, in standard form, is equal to $\Delta h / \Delta dh$.

PROOF. Let $L = \gcd(h_0, h_1)$ be in standard form. Then L is that unique common divisor of h_0 and h_1 which is in standard form and has maximum norm. Thus $L = I$ or $NL = p$. Assume $NL = p$. By Theorem 1, $f = L$ is a common root of the two polynomial equations

$$P_i(f) := f^2 - f * dh_i + h_i = 0, \quad (i = 0, 1).$$

Taking the difference of these two equations, we get

$$\Delta dh * L - \Delta h = 0.$$

Since $\Delta h \neq 0$, then this last equation yields $\Delta dh | \Delta h$, and so $L = \Delta h / \Delta dh$ is a differential rational form in h_0, h_1 . Also, $\Delta h / \Delta dh$ must be a root of each of the two polynomial equations in (1).

Conversely, assume h_0, h_1 satisfy (1). Then $\Delta dh \neq 0$, and the element $\Delta h / \Delta dh$ in the field of quotients of Λ is a root of the two polynomial equations in (1). Since these equations are monic, then $\Delta h / \Delta dh$ belongs to Λ , and by Theorem 1, $\Delta h / \Delta dh$ is a common divisor of h_0, h_1 in standard form and of norm p . \square

THEOREM 5. *There is no differential polynomial in h_0, h_1 which is equal to the greatest common divisor of h_0, h_1 , in standard form, whenever h_0 and h_1 are of norm p^2 , in standard form and the greatest common divisor is of norm p .*

PROOF. Define

$$h_x(n) = (1 - x)h_0(n) + xh_1(n),$$

where x is a numerical parameter. It is easily checked that, for every x , the function h_x is in standard form and has the same norm as h_0 and h_1 . Also, $L := \gcd(h_0, h_x) = \gcd(h_0, h_1) = \gcd(h_1, h_x)$ whenever $x \neq 0$.

Suppose there exists a differential polynomial as described in the statements of the theorem. In this expression, replace h_1 by $h_x := h_0 + x\Delta h$, and dh_1 by $dh_0 + x\Delta dh$. For fixed n , the value of this expression is a polynomial in x which is equal to $L(n)$ for each $x \neq 0$. Thus L is equal to the sum of the terms of the differential polynomial not containing x , i.e. not containing Δh nor Δdh . Consequently, $L = \gcd(h_0, h_1)$ is representable by a formula independent of h_1 , which is absurd. \square

THEOREM 6. *Let h_0, h_1 be in standard form, with $Nh_0 = p^2$, $Nh_1 = p^3$, $h_0 \nmid h_1$. Then $L := \gcd(h_0, h_1)$, in standard form, is either I of norm 1, or*

$$\frac{h_0 * dh_0 - \frac{1}{2}h_0 * d^2h_1 + h_1}{(dh_0)^2 - \frac{1}{2}dh_0 * d^2h_1 + dh_1 - h_0}$$

of norm p .

PROOF. Since $h_0 \nmid h_1$, then L must be I or of norm p . In the latter case, $f = L$, by Theorem 1, is a common root of the quadratic polynomial

$$f^2 - f * dh_0 + h_0 = 0$$

and of the cubic polynomial

$$f^3 - \frac{1}{2}f^2 * d^2h_1 + f * dh_1 - h_1 = 0.$$

Dividing the former into the latter, we get a linear remainder

$$\left((dh_0)^2 - \frac{1}{2}dh_0 * d^2h_1 + dh_1 - h_0 \right) * f - \left(h_0 * dh_0 - \frac{1}{2}h_0 * d^2h_1 + h_1 \right)$$

for which L is also a root. Thus there is just one possible value for L , and it is a differential rational form in h_0, h_1 . \square

THEOREM 7. Let h_0, h_1 be in standard form, not equal, each of norm p^3 . Then $L := \gcd(h_0, h_1)$ is either I of norm 1, or $2\Delta h / \Delta d^2h$ of norm p^2 , or

$$\frac{4\Delta h * \Delta dh - \Delta d^2h * (d^2h_0 * h_1 - h_0 * d^2h_1)}{4(\Delta dh)^2 + \Delta d^2h * (dh_0 * d^2h_1 - d^2h_0 * dh_1 - \Delta h)}$$

of norm p .

PROOF. If $L \neq I$, then $NL = p^2$ or p . We consider each case separately.

Case $NL = p^2$. By Theorem 3, $f = L$ is a common root of the cubic polynomial

$$f^3 - dh_i * f^2 + \frac{1}{2}d^2h_i * h_i * f - h_i^2 = 0 \quad (i = 0, 1). \quad (2)$$

As in the proof of Theorem 5, let $h_x = (1-x)h_0 + xh_1 = h_0 + x\Delta h$. Note that L is also a root of (2) with $i = x$. Equating the coefficients of x^2 in (2), we get $L = \frac{2\Delta h}{\Delta d^2h}$.

Case $NL = p$. By Theorem 1, L is a common root of the two cubic polynomial equations

$$0 = f^3 - \frac{1}{2}f^2 * d^2h_i + f * dh_i - h_i \quad (i = 0, 1). \quad (3)$$

Taking the difference, we have

$$\frac{1}{2}f^2 * \Delta d^2h - f * \Delta dh + \Delta h = 0, \quad (4)$$

of which L is also a root. If $\Delta d^2h = 0$, then $L = \frac{\Delta h}{\Delta dh}$. If $\Delta d^2h \neq 0$, divide the quadratic polynomial (4) into (3) corresponding to h_0 , the constant term of the linear remainder, apart from the nonzero factor $\frac{1}{(\Delta d^2h)^2}$, is

$$-4\Delta h * \Delta dh + d^2h_0 * \Delta h * \Delta d^2h - h_0 * (\Delta d^2h)^2. \quad (5)$$

We shall show that this expression is nonzero. This will imply that the linear remainder is not identically zero, and since its coefficients are differential rational forms, and L is its root, we then obtain a differential form for L .

Assume (5) is zero and $\Delta d^2 h \neq 0$. Divide (5) by L and rewrite it as

$$\frac{h_0 * (\Delta d^2 h)^2}{L} = (d^2 h_0 * \Delta d^2 h - 4\Delta dh) * \frac{\Delta h}{L}.$$

Since $\frac{h_0}{L}$ and $\frac{\Delta h}{L}$ are relatively prime, the former divides $d^2 h_0 * \Delta d^2 h - 4\Delta dh$. This last quantity is not zero but has zero second derivation, which contradicts the fact that it is divisible by $\frac{h_0}{L}$, of norm p^2 . Solving the linear remainder for L , we get the required result. \square

THEOREM 8. *Let h_0, h_1 be in standard form, each having norm equal to a power of p not exceeding p^4 . Then L is always expressible as a differential rational form in h_0 and h_1 .*

PROOF. We may assume that $Nh_0 = Nh_1 = p^4$. For if each norm is less than p^4 , the result follows from Theorems 4, 6 and 7, and if $Nh_0 = p^4, Nh_1 = p^c$, c being less than 4, and the theorem has been proved for $L' = \gcd(h_0, r^{4-c} * h_1)$, r being as defined in the proof of Theorem 1, then the result is also true for $L = \gcd(h_0, h_1)$, because L is either equal to L' or to L' divided by a power of r , since r is a prime in Λ . We may further assume $h_0 \neq h_1, L \neq I$, so NL is either p^3, p^2 or p .

Case $NL = p^3$. L is a common root, by Theorem 3, of the two quartic polynomial equations

$$f^4 - dh_i * f^3 + \frac{1}{2}d^2 h_i * h_i * f^2 - \frac{1}{6}d^3 h_i * h_i^2 * f + h_i^3 = 0 \quad (i = 0, 1).$$

Applying the h_x -method, as in Theorem 5, to these equations, and equating the x^3 -component, we get $L = \frac{\delta \Delta h}{\Delta d^3 h}$.

Case $NL = p$. By Theorem 1, L is a common root of the two quartic polynomial equations

$$f^4 - \frac{1}{3!}f^3 * d^3 h_i + \frac{1}{2!}f^2 * d^2 h_i - f * dh_i + h_i = 0 \quad (i = 0, 1). \quad (6)$$

Forming the difference of these two equations yields

$$-\frac{1}{6}f^3 * \Delta d^3 h + \frac{1}{2}f^2 * \Delta d^2 h - f * \Delta dh + \Delta h = 0, \quad (7)$$

of which L is also a root. If $\Delta d^2 h = 0$, then $L = \frac{\Delta h}{\Delta dh}$. If $\Delta d^3 h = 0$ and $\Delta d^2 h \neq 0$, then (7) reduces to (4). Dividing the quadratic polynomial (4) into the quartic polynomial (6) corresponding to h_0 , we obtain a linear remainder whose constant term, apart from a non-zero factor $\frac{1}{(\Delta d^2 h)^3}$, is of the form $h_0 * (\Delta d^2 h)^3 - 2J * \Delta h$, where

$$J = 4(\Delta dh)^2 - \frac{2}{3!}d^3 h_0 * \Delta dh * \Delta d^2 h - 2\Delta h * \Delta d^2 h + \frac{1}{2}d^2 h_0 * (\Delta d^2 h)^2$$

is a differential polynomial having zero third order derivation. We claim that this constant term is nonzero, for otherwise $\frac{h_0}{L} * (\Delta d^2 h)^3 = 2J * \frac{\Delta h}{L}$. Since $\frac{h_0}{L}$ and $\frac{\Delta h}{L}$ are relatively prime, then $\frac{h_0}{L}$ divides J . But $N(\frac{h_0}{L}) = p^3$ contradicting the fact that $d^3 J = 0$. Consequently, the linear (remainder) term is not zero, and as L is its root, we obtain a differential rational form for L . If $\Delta d^3 h \neq 0$, divide the cubic polynomial (7) into the quartic polynomial (6) corresponding to h_0 . The quadratic remainder R has a constant term, apart from the nonzero factor $\frac{J}{(\Delta d^3 h)^2}$, equal to $h_0 * (\Delta d^3 h)^2 + J' * \Delta h$, where $J' = 18\Delta d^2 h - d^3 h_0 * \Delta d^3 h$. We claim that this constant term is nonzero, for otherwise, we would have $\frac{h_0}{L} * (\Delta d^3 h)^2 = -J * \frac{\Delta h}{L}$. Since $\frac{h_0}{L}$ and $\frac{\Delta h}{L}$ are relatively prime, then $\frac{h_0}{L}$ divides J . Observe that $d^3 J = 0$, and $N(\frac{h_0}{L}) = p^3$, which is a contradiction. Thus the quadratic remainder term $R \neq 0$. If R is linear, we are through because its coefficients are differential rational forms and its root is L . Suppose R is of degree 2, with the second root f_0 belonging to the field of quotients of Λ . We may assume that f_0 is also a common root of the two polynomials (6) corresponding to h_0, h_1 , for otherwise division of R into one of these polynomials will produce a linear polynomial with differential rational forms as coefficients having L as its root, and we are done. Since (6) is monic, f_0 then belongs to Λ , and by Theorem 1, f_0 is a common divisor of h_0, h_1 , of norm p , and in standard form. Thus $f_0 = L$, so L is a double root of R . Therefore, the discriminant of R is 0. We thus obtain a differential rational form for L .

Case $NL = p^2$. By Lemma 6, $f = L$ is a root of $T(f) = 0$, with h replaced by $h_x := (1-x)h_0 + xh_1$. The coefficient of x^3 in $T(f)$, after cancelling the nonzero factor Δh , is equal to

$$V(f) := (\Delta h)^2 - \frac{1}{2} \Delta h * \Delta d^2 h * f + \frac{1}{6} \Delta dh * \Delta d^3 h * f^2 - \frac{1}{36} * (\Delta d^3 h)^2 * f^3,$$

and L is a root of $V(f) = 0$. If $\Delta d^3 h = 0$, we get $L = \frac{2\Delta h}{\Delta d^2 h}$, and we are done. We thus assume $\Delta d^3 h \neq 0$. The coefficient of x^2 in $T(f)$ is

$$\begin{aligned} & 3h_0 * (\Delta h)^2 - \frac{1}{2} f * (2h_0 * \Delta h * \Delta d^2 h + d^2 h_0 * (\Delta h)^2) + f^2 * \left(\frac{1}{6} h_0 * \Delta dh \right. \\ & \quad \left. * \Delta d^3 h - (\Delta h)^2 + \frac{1}{6} \Delta h * \Delta dh * d^3 h_0 + \frac{1}{6} dh_0 * \Delta h * \Delta d^3 h \right) \\ & + f^3 * \left(-(\Delta dh)^2 - \frac{1}{36} (h_0 * (\Delta d^3 h)^2 + 2d^3 h_0 * \Delta h * \Delta d^3 h) + \Delta h * \Delta d^2 h \right) \\ & + f^4 * \left(\frac{1}{6} \Delta dh * d^3 h \right), \end{aligned}$$

which is a quartic polynomial in f , and the remainder W , when divided by the cubic polynomial $V(f)$ has constant term equal to

$$\frac{2(\Delta h)^2}{(\Delta d^3 h)^2} (h_0 * (\Delta d^3 h)^2 + 18\Delta h * \Delta d^2 h - d^3 h_0 * \Delta h * \Delta d^3 h).$$

Apart from the nonzero factor $\frac{2(\Delta h)^2}{(\Delta d^3 h)^2}$, this constant term is exactly (8). Proceeding as after (8), we have that this constant term is nonzero. Thus the remainder W is a linear or quadratic polynomial with nonzero constant term, and having L as a root. If W is linear, then clearly L is expressible as a differential rational form in h_0, h_1 and we are through. Assume then that W is of degree 2, with second root f_1 belonging to the field of quotients of Λ . We may assume that f_1 is also a common root of the two polynomials $T(f)$ corresponding to h_0, h_1 , and also a root of $V(f)$, for otherwise division of W into one of these three polynomials will produce a linear polynomial with differential rational form coefficients having L as a root, and we are done. Since $T(f)$ is monic, f_1 thus belongs to Λ , and so by Lemma 6, f_1 is a common divisor of h_0, h_1 of norm p^2 . Also, since f_1 is a root of $V(f) = 0$, we know by Lemma 5 that $d^2 f_1 = 3!I$, so $\frac{1}{3}f_1$ is in standard form. Consequently, $f_1 = 3L$, and so L is a double root of W . Hence, the discriminant of W is 0, and we again obtain a differential rational form for L . \square

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
 [2] E. D. Cashwell and C. J. Everett, *The ring of number-theoretic functions*, Pacific J. Math., 9(1959), 975-985.
 [3] E. D. Cashwell and C. J. Everett, *Formal power series*, Pacific J. Math., 13(1963), 45-64.
 [4] David Rearick, *Divisibility of arithmetic functions*, Pacific J. Math., 112(1984), 237-248.
 [5] Harold N. Shapiro, *On the convolution ring of arithmetic functions*, Comm. Pure Appl. Math., 25(1972), 287-336.

บรรณานุกรม

1. T.M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York, 1976.
2. D.A. Buchsbaum, Some remarks on factorization in power series rings, J. Math. Mech. 10(5)(1961),749-753.
3. R. Bellman and H.N. Shapiro, The algebraic independence of arithmetic functions (I) Multiplicative functions, Duke Math. J. 15(1948),229-235.
4. E.D. Cashwell and C.J. Everett, The ring of number-theoretic functions, Pacific J. Math. 9(1959),975-985.
5. E.D. Cashwell and C.J. Everett, Formal power series, Pacific J. Math. 13(1963),45-64.
6. W. Krull, Beitrage zur Arithmetik kommutative Integritatsbereiche, III. Zum Dimensionsbegriff der Idealtheorie, Math. Zeit. 42(1937),745-766.
7. V. Laohakosol, K. Kongsakorn and U. Leerawat, Some arithmetic functions algebraically independent with respect to convolution, Soochow J. Math. 15(2)(1989),171-178.
8. J. Popken, Algebraic dependence of arithmetic functions, Proc. Kon. Ned. Akad. Wetensch. 65(1962),155-168.
9. D. Rearick, Divisibility of arithmetic functions, Pacific J. Math. 112(1984),237-248.
10. D. Rearick, Multiplicativity-preserving arithmetic power series, Pacific J. Math. 55(1)(1974),277-283.
11. W. Ruckert, Zum Eliminationsproblem der Potenzreihenideale, Math. Ann. 107(1933),259-281.
12. P. Samuel, On unique factorization domains, Ill. J. Math. 5(1961),1-17.
13. H.N. Shapiro, On the convolution ring of arithmetic functions, Comm. Pure Appl. Math. 25(1972),287-336.
14. H.N. Shapiro and C.H. Sparer, On algebraic independence of Dirichlet series, Comm. Pure Appl. Math. 39(1986),695-745.

ประวัตินักวิจัยและคณะ

หัวหน้าโครงการ นายวิเชียร เลาทโกศล B.Sc.(Hons.), M.Sc., Ph.D.

อาชีพ รับราชการ ตำแหน่ง รองศาสตราจารย์

หน่วยงาน ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

กทม. 10900

ผู้ร่วมงาน

1. น.ส.กรรณิกา คงสาคร วท.บ.(เกียรตินิยม) วท.ม.

อาชีพ รับราชการ ตำแหน่ง ผู้ช่วยศาสตราจารย์

หน่วยงาน ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

กทม. 10900

2. น.ส.อุษณีย์ สิริวัฒน์ วท.บ.(เกียรตินิยม) วท.ม. วท.ด.

อาชีพ รับราชการ ตำแหน่ง อาจารย์

หน่วยงาน ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

กทม. 10900

