รายงานการวิจัยฉบับสมบูรณ์

โครงการวิจัย : ระบบส่วนตกค้างบริบูรณ์ในสนามกำลังสองเชิงจินตภาพ

ผู้วิจัย : นายสุธน ตาดี
วท.ม. (คณิตศาสตร์)

สาขาวิชาคณิตศาสตร์ คณะวิทยาศาสตร์และเทคโนโลยี
ได้รับทุนอุดหนุนจากมหาวิทยาลัยราชภัฏเทพสตรี
ประจำปีงบประมาณ 2560

Explicit complete residue systems in a general quadratic field

Suton Tadee[1], Vichian Laohakosol[2] and Santad Damkaew[3]

[1]Department of Mathematics, Faculty of Science and Technology,
Thepsatri Rajabhat University, Lopburi 15000, Thailand
E-mail: suton.t@tru.ac.th

[2]Department of Mathematics, Faculty of Science,
Kasetsart University, Bangkok 10900, Thailand
E-mail: fscivil@ku.ac.th

[3]Department of Mathematics and Computer Science, Faculty of Science,
Chulalongkorn University, Bangkok 10330, Thailand
E-mail: s.damkaew@hotmail.com

Abstract

Bergum explicitly determined three representations for a complete residue system in the quadratic field $\mathbb{Q}\left(\sqrt{-3}\right)$ extending two earlier results in $\mathbb{Q}\left(\sqrt{-1}\right)$ and $\mathbb{Q}\left(\sqrt{-2}\right)$. Among these three representations, the first is simplest to derive, while the third is minimal in the sense that the sum of their absolute values is minimal. Here, we extend these results by deriving explicit representations for a complete residue system in any general quadratic field. The first representation uses lattice points in a rectangle in the first quadrant of an appropriate plane, while the second representation uses lattice points in a parallelogram, and the third representation uses lattice points in a hexagon and possesses a minimality property for imaginary quadratic fields.

Key words and phrase: quadratic field, complete residue system, lattice point

คำนำ

โครงการวิจัย เรื่อง ระบบส่วนตกค้างบริบูรณ์ในสนามกำลังสองเชิงจินตภาพ จัดทำขึ้นโดยมีวัตถุประสงค์ 2 ประการ ประการแรก ศึกษาลักษณะและสมบัติของสมาชิกของริงของจำนวนเต็มเชิงพีชคณิตและระบบส่วนตกค้างบริบูรณ์ ประการที่สอง เพื่อหาระบบส่วนตกค้างบริบูรณ์ของ $\mathbb{Z}\left(\sqrt{m}\right)$ เมื่อ m เป็นจำนวนเต็มลบ และ $m \equiv 1 (\mathrm{mod}\ 4)$

โดยผลการวิจัยในครั้งนี้เป็นการสร้างองค์ความรู้ใหม่ทางด้านวิชาทฤษฎีจำนวน ซึ่งถือได้ว่าเป็นสาขาวิชาหนึ่งที่มีความสำคัญทางคณิตศาสตร์ นอกจากนี้องค์ความรู้ที่ได้รับยังมีส่วนช่วยพัฒนาความรู้และหลักการคิดค้นทฤษฎีบทพร้อมการพิสูจน์อย่างสมเหตุสมผลและรัดกุม เพื่อเป็นพื้นฐานในการนำไปประยุกต์ใช้ต่อไป

ผู้วิจัยหวังเป็นอย่างยิ่งว่าการวิจัยในครั้งนี้ จะเป็นประโยชน์ต่อ ครู อาจารย์ นักเรียน นักศึกษาหรือผู้ที่เกี่ยวข้องทั้งหลายและ หากเกิดข้อพกพร่อง ผู้วิจัยพร้อมที่จะรับข้อเสนอแนะ เพื่อที่จะนำมาปรับปรุงแก้ไขและพัฒนาเพื่อเกิดประโยชน์สูงสุดต่อการศึกษาของประเทศไทยต่อไป

สุธน ตาดี

กิตติกรรมประกาศ

โครงการวิจัย เรื่อง ระบบส่วนตกค้างบริบูรณ์ในสนามกำลังสองเชิงจินตภาพ สำเร็จลงด้วยดี เพราะได้รับความกรุณาจากหลายฝ่าย ผู้วิจัยขอขอบคุณมหาวิทยาลัยราชภัฏเทพสตรีที่ให้ทุนอุดหนุนงานวิจัยในครั้งนี้

ขอขอบคุณ ศ.ดร.วิเชียร เลาหโกศล อาจารย์ประจำภาควิชาคณิตศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ ที่ได้ประสิทธิ์ประสาทวิชาความรู้และให้คำปรึกษาอย่างดียิ่ง ผู้วิจัยยึดถือเป็นแบบอย่างตลอดมา และขอขอบคุณ คณบดีคณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏเทพสตรี ที่ได้ให้การสนับสนุนการดำเนินงานโครงการวิจัย ผู้วิจัยขอขอบคุณทุกท่านที่กล่าวมา ณ โอกาสนี้อีกครั้งหนึ่ง

สุธน ตาดี

สารบัญ

รายงานการวิจัยฉบับสมบูรณ์
ทุนอุดหนุนการวิจัยปีงบประมาณ พ.ศ. 2560
มหาวิทยาลัยราชภัฏเทพสตรี

---

1. ชื่อโครงการ

(ภาษาไทย) ระบบส่วนตกค้างบริบูรณ์ในสนามกำลังสองเชิงจินตภาพ

(ภาษาอังกฤษ) Complete residue systems in imaginary quadratic fields

2. ประเภทงานวิจัย

☑ การวิจัยพื้นฐาน (Basic research)

☐ การวิจัยประยุกต์ (Applied research)

☐ การพัฒนาทดลอง (Experimental development)

3. สาขาวิชาที่ทำการวิจัย

สาขาวิชาวิทยาศาสตร์กายภาพและคณิตศาสตร์ กลุ่มวิชาคณิตศาสตร์และสถิติ

4. คำสำคัญ (keywords) ของการวิจัย

สนามกำลังสอง (Quadratic field), ระบบส่วนตกค้างบริบูรณ์ (Complete residue systems), จุดแลคทิช (Lattice point)

5. คณะผู้วิจัย

5.1 หัวหน้าโครงการวิจัย

ชื่อ – นามสกุล	นายสุธน ตาดี
ตำแหน่ง	อาจารย์
หน่วยงานที่สังกัด	สาขาวิชาคณิตศาสตร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏเทพสตรี
หมายเลขโทรศัพท์	081-9040975
E-mail	suton.t@tru.ac.th

5.2 ที่ปรึกษาโครงการวิจัย

ชื่อ - นามสกุล	ดร.วิเชียร เลาหโกศล
ตำแหน่ง	ศาสตราจารย์
หน่วยงานที่สังกัด	ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์
หมายเลขโทรศัพท์	081-4779192
E-mail	fscivil@ku.ac.th

5.3 ผู้ร่วมวิจัย

ชื่อ - นามสกุล	นายสันทัด แดงแก้ว
ตำแหน่ง	นักศึกษา (ปริญญาโท)
หน่วยงานที่สังกัด	ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
หมายเลขโทรศัพท์	086-6925319
E-mail	s.damkaew@hotmail.co.th

6. ความสำคัญและที่มาของปัญหาการวิจัย

ในปีงบประมาณ 2559 ผู้วิจัยได้รับทุนสนับสนุนการวิจัยเพื่อสร้างองค์ความรู้ จากมหาวิทยาลัยราชภัฏเทพสตรี ชื่อโครงการวิจัย "ระบบส่วนตกค้างบริบูรณ์ในสามโดเมนแบบยูคลิกกำลังสองเชิงซ้อน" โดยศึกษาและดำเนินการพิสูจน์ทฤษฎีบทต่างๆ เพื่อหาระบบส่วนตกค้างบริบูรณ์ในโดเมนแบบยูคลิกกำลังสองเชิงซ้อน (Complex quadratic Euclidean domains) ในริงของจำนวนเต็มเชิงพีชคณิต $\mathbb{Z}\left(\sqrt{m}\right)$ สำหรับ $m=-3,-7,-11$

หลังจากที่ได้ทฤษฎีบทและวิธีพิสูจน์แล้ว ผู้วิจัยสังเกตเห็นว่า ทฤษฎีบทและวิธีพิสูจน์ดังกล่าวสามารถนำไปประยุกต์ใช้สำหรับริงของจำนวนเต็มเชิงพีชคณิต $\mathbb{Z}\left(\sqrt{m}\right)$ เมื่อ m เป็นจำนวนเต็มลบ และ $m \equiv 1 \pmod 4$ โดยเพิ่มเงื่อนไขบางอย่างและปรับเปลี่ยนการพิสูจน์ โดยเหตุนี้ผู้วิจัยจึงสนใจและเห็นความต่อเนื่องของงานวิจัยที่จะนำไปสู่องค์ความรู้ใหม่เพื่อพัฒนาผลงานดังกล่าวต่อไปในอนาคต

อนึ่ง เพื่อให้เกิดความเข้าใจในงานวิจัยนี้มากขึ้น ผู้วิจัยขอนำเสนอบทนิยามที่สำคัญต่องานวิจัย ดังมีรายละเอียดต่อไปนี้

บทนิยาม 6.1 ให้ a, b เป็นจำนวนเต็ม และ n เป็นจำนวนเต็มบวก เราจะกล่าวว่า a สมภาค หรือ คอนกรูเอนซ์ (Congruence) กับ b มอดุโล n เขียนแทนด้วย $a \equiv b \pmod n$ ก็ต่อเมื่อ n หาร $a-b$ ลงตัว

บทนิยาม 6.2 ให้ a, b เป็นจำนวนเต็ม และ n เป็นจำนวนเต็มบวก เราจะเรียก b ว่า เป็น ส่วนตกค้าง (Residue) ของ a มอดุโล n ถ้า $a \equiv b \pmod n$

เราจะเรียกเซตของจำนวนเต็ม $\{a_1, a_2, a_3, \ldots, a_n\}$ ว่าเป็น ระบบส่วนตกค้างบริบูรณ์ (Complete residue system) มอดุโล n ก็ต่อเมื่อ ทุกๆ จำนวนเต็ม a จะมี $a_i \in \{a_1, a_2, a_3, \ldots, a_n\}$ เพียงตัวเดียว ซึ่งทำให้

$$a \equiv a_i \pmod n$$

และเรียกเซต $\{a \in \mathbb{Z} : a \equiv a_i \pmod n\}$ ว่าชั้นส่วนตกค้าง (Residue class) ของ a_i มอดุโล n

หมายเหตุ ให้ x, q, r เป็นจำนวนเต็ม, n เป็นจำนวนเต็มบวก และ $x = nq + r$ ดังนั้น $x \equiv r \pmod{n}$ จะได้ว่า r เป็นส่วนตกค้าง (Residue) ของ x มอดุโล n และถ้า $0 \le r < n$ เราจะเรียก r ว่าเป็นส่วนตกค้างที่ไม่เป็นลบค่าน้อยสุด (Least non-negative residue) ของ x มอดุโล n เพราะฉะนั้น เซต $\{0, 1, 2, \ldots, n-1\}$ เรียกว่า ระบบส่วนตกค้างบริบูรณ์ที่ไม่เป็นลบค่าน้อยสุด (Least non-negative residue system) มอดุโล n นั่นคือ จะมี $r \in \{0, 1, 2, \ldots, n-1\}$ เพียงจำนวนเดียวเท่านั้นที่เป็นส่วนตกค้างของ x มอดุโล n

บทนิยาม 6.3 เราจะเรียกจำนวนเชิงซ้อน α ว่า จำนวนเชิงพีชคณิต (Algebraic number) ถ้า α เป็นรากของพหุนามที่มีสัมประสิทธิ์เป็นจำนวนเต็ม หรือ มีจำนวนเต็ม $a_0, a_1, a_2, a_3, \ldots, a_n$ ที่ไม่เป็นศูนย์พร้อมกัน ซึ่งทำให้

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

ถ้า α ไม่เป็นจำนวนเชิงพีชคณิต เราจะเรียก α ว่าจำนวนอดิศัย (Transcendental number)

บทนิยาม 6.4 เราจะเรียกจำนวนเชิงพีชคณิต α ว่าเป็นจำนวนเต็มเชิงพีชคณิต (Algebraic integer number) ถ้าสัมประสิทธิ์นำของสมการในบทนิยาม 6.3 เท่ากับ 1 หรือ $a_n = 1$

บทนิยาม 6.5 เราจะกล่าวว่าจำนวนเชิงพีชคณิต α มีดีกรี (Degree) n ถ้า α เป็นรากของพหุนามที่มีสัมประสิทธิ์เป็นจำนวนเต็มและมีดีกรี n และไม่เป็นรากของพหุนามที่มีสัมประสิทธิ์เป็นจำนวนเต็มและมีดีกรีต่ำกว่า n และเรียกพหุนามที่มีสัมประสิทธิ์เป็นจำนวนเต็มและมีดีกรี n ว่า Minimal polynomial ของ α

สัญลักษณ์ $\mathbb{Z}$ แทนเซตของจำนวนเต็ม
$\mathbb{Z}[x]$ แทนเซตของพหุนามที่มีสัมประสิทธิ์เป็นจำนวนเต็ม
$\deg f$ แทนดีกรี (Degree) ของพหุนาม $f(x)$

บทนิยาม 6.6 ให้ $f(x), g(x) \in \mathbb{Z}[x]$ โดยที่ $f(x) \neq 0$ เราจะกล่าวว่า $f(x)$ หาร $g(x)$ ลงตัว ถ้ามี $q(x) \in \mathbb{Z}[x]$ ซึ่งทำให้ $g(x) = f(x)q(x)$ และเรียก $f(x)$ ว่าตัวประกอบ (Factor) ของ $g(x)$ เขียนแทนด้วย $f(x) \mid g(x)$

บทนิยาม 6.7 สับฟิลด์ (Subfield) ของฟิลด์จำนวนเชิงพีชคณิต เราเรียกว่า ฟิลด์ของจำนวนเชิงพีชคณิต (Algebraic number field)

ให้ α เป็นจำนวนเชิงพีชคณิต จะได้ว่า เซตของจำนวนที่อยู่ในรูป $\frac{f(\alpha)}{g(\alpha)}$ โดยที่ $f(x), g(x) \in \mathbb{Z}[x]$ และ $g(\alpha) \neq 0$ เป็นฟิลด์ เขียนแทนด้วย $\mathbb{Z}(\alpha)$ เรียกว่า ส่วนขยาย (Extension) ของ $\mathbb{Z}$ ที่เกี่ยวเนื่องกับ α (by a formed by adjoining α to $\mathbb{Z}$)

บทนิยาม 6.8 ให้ α เป็นจำนวนเชิงพีชคณิต และ $f(x)$ เป็น Minimal polynomial โดยที่ $\deg f = n$ ถ้า $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ เป็นรากทั้งหมดที่แตกต่างกันของ $f(x)$ แล้ว $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ เป็นจำนวนเชิงพีชคณิต เราจะเรียก $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ ว่า สังยุค (Conjugate) ของ α

ถ้า $\xi \in \mathbb{Z}(\alpha)$ และ $\xi = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}$ แล้ว

$$\xi_i = a_0 + a_1\alpha_i + a_2\alpha_i^2 + \cdots + a_{n-1}\alpha_i^{n-1} \text{ สำหรับทุก } i = 1, 2, 3, \ldots, n-1$$

เราจะเรียก ξ_i ว่า Field conjugates ของ ξ

บทนิยาม 6.9 ให้ ξ เป็นจำนวนเชิงพีชคณิตใน $\mathbb{Z}(\alpha)$ ที่มีดีกรี n และให้ $\xi_1, \xi_2, \ldots, \xi_{n-1}$ เป็น Field conjugates ของ ξ เราจะเรียกผลคูณ $\xi_1\xi_2\cdots\xi_{n-1}$ ว่า Norm ของ ξ บน $\mathbb{Z}(\alpha)$ เขียนแทนด้วย $N(\xi)$

บทนิยาม 6.10 เราจะเรียก ริงของจำนวนเต็มเชิงพีชคณิตที่อยู่ในฟิลด์ $\mathbb{Z}(\alpha)$ ว่า Norm-Euclidean หรือ Euclidean domain ถ้า สำหรับทุก ξ_1 และ ξ_2 ที่เป็นสมาชิกในริงของจำนวนเต็มเชิงพีชคณิตที่อยู่ในฟิลด์ $\mathbb{Z}(\alpha)$ โดยที่ $\xi_2 \neq 0$ แล้วมี λ และ ρ ที่เป็นสมาชิกในริงของจำนวนเต็มเชิงพีชคณิตที่อยู่ในฟิลด์ $\mathbb{Z}(\alpha)$ ซึ่งทำให้ $\xi_1 = \xi_2\lambda + \rho$ โดยที่ $|N(\rho)| < |N(\xi_2)|$

จากบทนิยามข้างต้นเราสามารถนิยามการหารลงตัว (Divisibility) และสมภาค (Congruence) ในโดเมนแบบยุคลิด (Euclidean domain) ได้ดังนี้

ให้ α, δ และ γ เป็นสมาชิกของโดเมนแบบยูคลิก โดยที่ $\gamma \neq 0$ เราจะเรียกว่า

1. $\gamma \mid \alpha$ ก็ต่อเมื่อ มี β เป็นสมาชิกในโดเมนแบบยูคลิก ซึ่งทำให้ $\alpha = \gamma\beta$
2. $\alpha \equiv \delta \pmod{\gamma}$ ก็ต่อเมื่อ $\gamma \mid (\alpha - \delta)$

บทนิยาม 6.11 ถ้า $m > 0$ เราจะเรียก $\mathbb{Z}(\sqrt{m})$ ว่า Real quadratic field และถ้า $m < 0$ เราจะเรียก $\mathbb{Z}(\sqrt{m})$ ว่า Complex quadratic field

สำหรับงานวิจัยนี้ เราจะสนใจระบบส่วนตกค้างบริบูรณ์ในโดเมนแบบยูคลิกกำลังสองเชิงซ้อน (Complex quadratic Euclidean domains) ในอดีตนักคณิตศาสตร์ได้ศึกษาและค้นพบว่า ริงของจำนวนเต็มเชิงพีชคณิตที่อยู่ในฟิลด์ $\mathbb{Z}\left(\sqrt{m}\right)$ เป็น Complex quadratic Euclidean domains ก็ต่อเมื่อ $m=-1,-2,-3,-7,-11$ เท่านั้น และต่อมาได้มีผู้ศึกษาเกี่ยวกับเรื่องนี้ และได้ค้นพบระบบส่วนตกค้างบริบูรณ์ สำหรับ $m=-1,-2,-3$ แต่ยังไม่มีผู้ใดหาระบบส่วนตกค้างบริบูรณ์ สำหรับ $m=-7,-11$ ดังนั้นในงานวิจัยนี้เราจะหาระบบดังกล่าว โดยจะหาระบบส่วนตกค้างบริบูรณ์ในโดเมนแบบยูคลิกกำลังสองเชิงซ้อนตามแนวทางของ Bergum [1, หน้า 75 - 86] ที่หาระบบส่วนตกค้างบริบูรณ์ สำหรับ $m=-3$ ดังนั้น เราจะแสดงวิธีการหาระบบส่วนตกค้างบริบูรณ์ สำหรับ $m=-3,-7,-11$ ไปพร้อมกัน

ข้อตกลง เราทราบว่า $-\frac{1}{2}+\frac{\sqrt{m}}{2}$ เป็นจำนวนเต็มเชิงพีชคณิต (Algebraic integer) เมื่อ $m=-3,-7,-11$

กำหนดสัญลักษณ์ $\sigma_m=-\frac{1}{2}+\frac{\sqrt{m}}{2}$ เมื่อ $m=-3,-7,-11$

ให้ $\mathbb{Z}(\sigma_m)=\{a+b\sigma_m : a,b\in\mathbb{Z}\}$ และ $\gamma=a+b\sigma_m$

จะได้ว่า ขนาด (Norm) ของ γ (เขียนแทนด้วย $|\gamma|^2$)

$$|\gamma|^2=a^2-ab+\left(\frac{1-m}{4}\right)b^2$$

7. วัตถุประสงค์ของการวิจัย

7.1 ศึกษาลักษณะและสมบัติของสมาชิกของริงของจำนวนเต็มเชิงพีชคณิตและระบบส่วนตกค้างบริบูรณ์

7.2 เพื่อหาระบบส่วนตกค้างบริบูรณ์ของ $\mathbb{Z}\left(\sqrt{m}\right)$ เมื่อ m เป็นจำนวนเต็มลบ และ $m\equiv 1\pmod 4$

8. ขอบเขตของการวิจัย

ศึกษาเฉพาะระบบส่วนตกค้างบริบูรณ์ในสนามกำลังสองเชิงจินตภาพ

9. ทฤษฎี สมมติฐาน (ถ้ามี) และกรอบแนวความคิดของโครงการวิจัย

ทฤษฎีที่เกี่ยวข้องกับโครงการวิจัย [7, หน้า 639 - 690]:

ทฤษฎีบท 9.1 ขั้นตอนวิธีการหาร (The division algorithm)

ให้ a และ b เป็นจำนวนเต็มโดยที่ $a\neq 0$ จะได้ว่า มีจำนวนเต็ม q และ r เพียงคู่เดียวเท่านั้น ซึ่งทำให้

$$b=aq+r \text{ โดยที่ } 0\le r<|a|$$

จะเรียก q ว่า ผลหาร (Quotient) และ r ว่า เศษ (Remainder)

ทฤษฎีบท 9.2 จากบทนิยามข้างต้นจะได้ว่า

1. $\{0,1,2,\ldots,n-1\}$ และ $\{1,2,3,\ldots,n\}$ ต่างเป็นระบบส่วนตกค้างบริบูรณ์ มอดุโล n

2. ถ้า $\{a_1,a_2,a_3,\ldots,a_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n และ c เป็นจำนวนเต็ม แล้ว $\{a_1+c,a_2+c,a_3+c,\ldots,a_n+c\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n

3. ให้ $\{a_1,a_2,a_3,\ldots,a_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n จะได้ว่า สำหรับทุกๆ $a_i,a_j\in\{a_1,a_2,a_3,\ldots,a_n\}$ ถ้า $a_i\equiv a_j\pmod{n}$ แล้ว $a_i=a_j$

4. ถ้า $\{a_1,a_2,a_3,\ldots,a_n\}$ และ $\{b_1,b_2,b_3,\ldots,b_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n แล้ว สำหรับทุกๆ $a_i\in\{a_1,a_2,a_3,\ldots,a_n\}$ จะมี $b_j\in\{b_1,b_2,b_3,\ldots,b_n\}$ เพียงตัวเดียวเท่านั้น ซึ่งทำให้ $a_i\equiv b_j\pmod{n}$

5. ถ้า $\{a_1,a_2,a_3,\ldots,a_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n และ c เป็นจำนวนเต็ม โดยที่ ห.ร.ม. ของ c และ n เท่ากับ 1 แล้ว $\{ca_1,ca_2,ca_3,\ \ldots\ ,ca_n\}$ เป็นระบบส่วนตกค้างบริบูรณ์มอดุโล n

ทฤษฎีบท 9.3

1. ถ้า r เป็นจำนวนตรรกยะ แล้ว r เป็นจำนวนเชิงพีชคณิต

2. ถ้า a,b,c และ m เป็นจำนวนเต็ม โดยที่ $c\neq 0$ แล้ว $\dfrac{a+b\sqrt{m}}{c}$ เป็นจำนวนเชิงพีชคณิต

ทฤษฎีบท 9.4

1. ถ้า α และ β เป็นจำนวนเชิงพีชคณิต แล้ว $\alpha+\beta$ และ $\alpha\beta$ เป็นจำนวนพีชคณิต

2. ถ้า α และ β เป็นจำนวนเต็มเชิงพีชคณิต แล้ว $\alpha+\beta$ และ $\alpha\beta$ เป็นจำนวนเต็มเชิงพีชคณิต

ทฤษฎีบท 9.5 เซตของจำนวนเชิงพีชคณิตเป็นฟีลด์ (Field) และเซตของจำนวนเต็มเชิงพีชคณิตเป็นริง (Ring)

ทฤษฎีบท 9.6

1. ถ้า ξ เป็นจำนวนเชิงพีชคณิต แล้ว $N(\xi)$ เป็นจำนวนตรรกยะ

2. ถ้า ξ เป็นจำนวนเต็มเชิงพีชคณิต แล้ว $N(\xi)$ เป็นจำนวนเต็ม

ทฤษฎีบท 9.7 ให้ ξ_1 และ ξ_2 เป็นจำนวนเชิงพีชคณิตใน $\mathbb{Z}(\alpha)$ จะได้ว่า

1. $N(\xi_1\xi_2)=N(\xi_1)N(\xi_2)$

2. $N(\xi_1)=0$ ก็ต่อเมื่อ $\xi_1=0$

3. ถ้า $\xi_2\neq 0$ แล้ว $N\left(\dfrac{\xi_1}{\xi_2}\right)=\dfrac{N(\xi_1)}{N(\xi_2)}$

ทฤษฎีบท 9.8 ทุกริงของจำนวนเต็มเชิงพีชคณิตที่อยู่ในฟีลด์ $\mathbb{Z}(\alpha)$ ที่เป็น Euclidean domain จะเป็น unique factorization domain (UFD) ด้วย

ทฤษฎีบท 9.9 ริงของจำนวนเต็มเชิงพีชคณิตที่อยู่ในฟิลด์ $\mathbb{Z}\left(\sqrt{m}\right)$ เป็น Complex quadratic Euclidean domains ก็ต่อเมื่อ $m=-1,-2,-3,-7,-11$

บทแทรก 9.10 ถ้า $m=-1,-2,-3,-7,-11$ แล้ว ริงของจำนวนเต็มเชิงพีชคณิตที่อยู่ในฟิลด์ $\mathbb{Z}\left(\sqrt{m}\right)$ เป็น Unique factorization domain (UFD)

สมมุติฐานของโครงการวิจัย: การหาระบบส่วนตกค้างบริบูรณ์ของ $\mathbb{Z}\left(\sqrt{m}\right)$ เมื่อ m เป็นจำนวนเต็มลบ และ $m\equiv 1\,(\mathrm{mod}\,4)$ สามารถหาได้ในทำนองเดียวกับระบบส่วนตกค้างบริบูรณ์ ใน $\mathbb{Z}(\sigma_{-3})$, $\mathbb{Z}(\sigma_{-7})$ และ $\mathbb{Z}(\sigma_{-11})$ หรือกล่าวอีกนัยหนึ่ง คือ เราสามารถใช้แนวทางในการพิสูจน์ของ Bergum [1, หน้า 75 - 86] มาขยายผลเพื่อหาระบบส่วนตกค้างบริบูรณ์ ใน $\mathbb{Z}\left(\sqrt{m}\right)$ เมื่อ m เป็นจำนวนเต็มลบ และ $m\equiv 1\,(\mathrm{mod}\,4)$ ได้

กรอบแนวความคิดของโครงการวิจัย: เราจะค้นคว้าและศึกษาสมบัติและทฤษฎีต่างๆ ที่เกี่ยวข้องกับจำนวนเชิงพีชคณิต (Algebraic number) ระบบส่วนตกค้างบริบูรณ์ (Complete residue system) และสนามกำลังสองเชิงจินตภาพ (Imaginary quadratic field) พร้อมกับศึกษาการพิสูจน์ของ Bergum [1, หน้า 75 - 86] อย่างละเอียด จากนั้นนำความรู้ที่ได้มาบูรณาการเข้าด้วยกัน วิเคราะห์และสังเคราะห์หาระบบส่วนตกค้างบริบูรณ์ ตามที่ได้ตั้งสมมุติฐานไว้

10. การทบทวนวรรณกรรม/สารสนเทศ (information) ที่เกี่ยวข้อง

ในปี ค.ศ. 1939 Uspensky และ Heaslet [8] ได้พบหลายตัวแทนของระบบส่วนตกค้างบริบูรณ์มอดุโล n เมื่อ n เป็นจำนวนเต็มที่ไม่เท่ากับศูนย์ และสองระบบส่วนตกค้างบริบูรณ์มอดุโล n ที่เป็นที่รู้จักเป็นอย่างดี คือ เซตของจำนวนเต็ม $\{0,1,2,\ldots,n-1\}$ และเซตของจำนวนเต็ม $\left\{x\in\mathbb{Z}:-\frac{n}{2}<x\leq\frac{n}{2}\right\}$

ในปี ค.ศ. 1965 Jordan และ Potratz [3, หน้า 1 - 12] ได้ตีพิมพ์ผลงานเกี่ยวกับหลายตัวแทนของระบบส่วนตกค้างบริบูรณ์ ในจำนวนเต็มของเกาส์ $\mathbb{Z}\left(\sqrt{-1}\right)=\left\{a+b\sqrt{-1}:\ a,b\in\mathbb{Z}\right\}$ ซึ่งต่อมาในปี ค.ศ. 1966 Potratz [6] ได้ขยายงานวิจัยและค้นพบหลายตัวแทนของระบบส่วนตกค้างบริบูรณ์ในโดเมนแบบยูคลิกกำลังสอง (Quadratic Euclidean domain) ของ $\mathbb{Z}\left(\sqrt{-2}\right)=\left\{a+b\sqrt{-2}:\ a,b\in\mathbb{Z}\right\}$

ในปี ค.ศ. 1978 Bergum [1, หน้า 75 - 86] ได้พบตัวแทนของระบบส่วนตกค้างบริบูรณ์ใน $\mathbb{Z}(\sigma_{-3})$ มี 3 แบบ ดังนี้

แบบที่ 1. ให้ $\gamma = a + b\sqrt{-3}$, $d = (a, b)$ และ $\gamma = d\left(a_1 + b_1\sqrt{-3}\right) = d\mu$

ทฤษฎีบท 10.1 ถ้า d เป็นจำนวนเต็มคู่

$$T_1 = \left\{ x + y\sqrt{-3} : 0 \le x \le d|\mu|^2 - 1, 0 \le y \le \frac{d-2}{2} \right\}$$

และ

$$T_2 = \left\{ \left(x + \frac{1}{2}\right) + \left(y + \frac{1}{2}\right)\sqrt{-3} : 0 \le x \le d|\mu|^2 - 1, 0 \le y \le \frac{d-2}{2} \right\}$$

แล้ว $T = T_1 \cup T_2$ เป็นตัวแทนของระบบส่วนตกค้างบริบูรณ์มอดุโล γ

ทฤษฎีบท 10.2 ถ้า d เป็นจำนวนเต็มคี่

$$T_1 = \left\{ x + y\sqrt{-3} : 0 \le x \le d|\mu|^2 - 1, 0 \le y \le \frac{d-1}{2} \right\}$$

และ

$$T_2 = \left\{ \left(x + \frac{1}{2}\right) + \left(y + \frac{1}{2}\right)\sqrt{-3} : 0 \le x \le d|\mu|^2 - 1, 0 \le y \le \frac{d-3}{2} \right\}$$

แล้ว $T = T_1 \cup T_2$ เป็นตัวแทนของระบบส่วนตกค้างบริบูรณ์มอดุโล γ

บทแทรก 10.3 จำนวนเชิงการนับ (Cardinality) ระบบส่วนตกค้างบริบูรณ์มอดุโล γ เท่ากับ $|\gamma|^2$

แบบที่ 2. ให้ $\gamma = a + b\sqrt{-3}$ และ

T_1 เป็นเซตที่รวบรวมจุดในรูปสี่เหลี่ยมขนมเปียกปูน (Rhombus) ABCD โดยมีจุดยอด (Vertices) คือ

$$\frac{\left(1+\sqrt{-3}\right)\gamma}{2}, \frac{\left(1-\sqrt{-3}\right)\gamma}{2}, \frac{\left(-1-\sqrt{-3}\right)\gamma}{2} \text{ และ } \frac{\left(-1+\sqrt{-3}\right)\gamma}{2}$$

และให้ T_2 เป็นเซตที่รวบรวมจุดบน The half-open line segments $\left(\frac{\pm\left(-1+\sqrt{-3}\right)\gamma}{2}, \frac{\left(-1-\sqrt{-3}\right)\gamma}{2} \right)$

ทฤษฎีบท 10.4 ให้ $T = T_1 \cup T_2$ จะได้ว่า T เป็นตัวแทนของระบบส่วนตกค้างบริบูรณ์มอดุโล γ

ทฤษฎีบท 10.5 ถ้า $\gamma = a + b\sqrt{-3}$ จะได้ว่า 2 หาร $|\gamma|^2$ ลงตัว ก็ต่อเมื่อ 2 หาร γ ลงตัว

ทฤษฎีบท 10.6 ให้ $\gamma = a + b\sqrt{-3}$ และ $T = T_1 \cup T_2$ จะได้ว่า เซต T_2 ไม่ว่าง ก็ต่อเมื่อ 2 หาร γ ไม่ลงตัว

แบบที่ 3. เราจะเรียกตัวแทน T ของระบบส่วนตกค้างบริบูรณ์มอดุโล γ เรียกว่า Absolute minimal representation ก็ต่อเมื่อ สำหรับตัวแทน R ใดๆ ของระบบส่วนตกค้างบริบูรณ์มอดุโล γ ซึ่งทำให้

$$\sum_{\alpha\in T}|\alpha| \le \sum_{\beta\in R}|\beta|$$

ให้ T_1 เป็นเซตของจุดภายใน (Points interior) the hexagon ABCDEF โดยที่ vertices คือ

$$\frac{\gamma\left(1-\sqrt{-3}\right)e^{\pi ki/3}}{3} \quad \text{เมื่อ } 1\le k\le 6$$

ให้ T_2 เป็นเซตของจุดบน The line segments

$$\left[-\frac{\gamma\left(1-\sqrt{-3}\right)}{3},\frac{\gamma\left(1-\sqrt{-3}\right)e^{4\pi i/3}}{3}\right],\left[\frac{\gamma\left(1-\sqrt{-3}\right)e^{4\pi i/3}}{3},\frac{\gamma\left(1-\sqrt{-3}\right)e^{5\pi i/3}}{3}\right]$$

และ

$$\left[\frac{\gamma\left(1-\sqrt{-3}\right)e^{5\pi i/3}}{3},\frac{\gamma\left(1-\sqrt{-3}\right)}{3}\right)$$

ทฤษฎีบท 10.7 $T=T_1\cup T_2$ เป็นตัวแทนของระบบส่วนตกค้างบริบูรณ์มอดุโล γ

บทตั้ง 10.8 ถ้า $-1\le a<1$ หรือ $-1<a\le 1$ และ r เป็นจำนวนเต็มใดๆ แล้ว $0\le r^2+ar$

บทตั้ง 10.9 ถ้า $\alpha\in T$ แล้ว $|\alpha|\le|\beta|$ สำหรับทุก $\beta\equiv\alpha\left(\mathrm{mod}\,\gamma\right)$

11. เอกสารอ้างอิงของโครงการวิจัย

[1] Bergum, G. E. Complete residue systems in the quadratic domain $\mathbb{Z}\left(e^{2\pi i/3}\right)$, Internat. J. Math" & Math. Sci. 1(1978), pp. 75 - 86.

[2] Hardman, N. R. and J. H. Jordan. A minimum problem connected with complete residue systems in the Gaussian integer, Amer. Math. Monthly 74(1967), pp. 559 - 561.

[3] Jordan, J. H. and C. J. Potratz. Complete residue systems in the Gaussian integer, Math. Mag. 38(1965), pp. 1 - 12.

[4] Hardy, G. H. and E.M. Wright, An Introduction to the Theory of Numbers, 4thedition, Oxford University Press, London, 1971.

[5] Niven, I., H.S. Zuckerman and H.L. Montgomery, An Introduction to the Theory of Numbers, 5th ed., John Wiley and Sons, New York, 1991.

[6] Potratz, C. J. Character sums in $\mathbb{Z}\left(\sqrt{2}\right)/(p)$. Unpublished Ph.D. dissertation, Washington State University, 1966.

[7] Redmond, D. Number theory : an introduction , Marcel Dekker. New York. 1996.

[8] Uspensky, J. V. and M. A. Heaslet. Elementary number theory, McGraw-Hill, New York, 1939.

12. วิธีการดำเนินการวิจัย และสถานที่ทำการทดลอง/เก็บข้อมูล

12.1 วิธีการดำเนินการวิจัย

1. ศึกษาค้นคว้าและรวบรวมผลงานวิจัยที่เกี่ยวข้องกับระบบส่วนตกค้างบริบูรณ์ในสนามกำลังสองเชิงจินตภาพ

2. เข้าร่วมประชุมสัมมนาเกี่ยวกับทฤษฎีจำนวนและการประยุกต์เพื่อให้ได้ข้อมูล แนวคิดใหม่ๆ และได้แลกเปลี่ยนความรู้กับผู้เชี่ยวชาญในสาขานี้

3. วิเคราะห์ระบบส่วนตกค้างบริบูรณ์ ใน $\mathbb{Z}\left(\sqrt{m}\right)$ เมื่อ m เป็นจำนวนเต็มลบ และ $m \equiv 1 \pmod 4$

4. ค้นหาระบบส่วนตกค้างบริบูรณ์ ใน $\mathbb{Z}\left(\sqrt{m}\right)$ เมื่อ m เป็นจำนวนเต็มลบ และ $m \equiv 1 \pmod 4$

5. สรุปผลการศึกษาวิจัย และส่งผลงานวิจัยไปยังวารสารวิชาการ

6. นำเสนอผลงานวิจัยในงานประชุมวิชาการทางด้านคณิตศาสตร์หรือเผยแพร่ผลงานวิจัยทางเว็ปไซต์ของมหาวิทยาลัย

12.2 สถานที่ทำการทดลอง/เก็บข้อมูล

1. สาขาวิชาคณิตศาสตร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏเทพสตรี
2. ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

13. ระยะเวลาทำการวิจัยและแผนการดำเนินงานตลอดโครงการวิจัย

การดำเนินงานวิจัย	ระยะเวลา											
	ต.ค. 59	พ.ย. 59	ธ.ค. 59	ม.ค. 60	ก.พ. 60	มี.ค. 60	เม.ย. 60	พ.ค. 60	มิ.ย. 60	ก.ค. 60	ส.ค. 60	ก.ย. 60
1. ศึกษาค้นคว้าและรวบรวมผลงานวิจัยที่เกี่ยวข้องกับระบบส่วนตกค้างบริบูรณ์ในสนามกำลังสองเชิงจินตภาพ	←	—	—	→								
2. เข้าร่วมประชุมเกี่ยวกับทฤษฎีจำนวนและการประยุกต์เพื่อให้ได้ข้อมูล แนวคิดใหม่ๆ และได้แลกเปลี่ยนความรู้กับผู้เชี่ยวชาญในสาขานี้					←	→						
3. วิเคราะห์ระบบส่วนตกค้างบริบูรณ์ ใน $\mathbb{Z}(\sqrt{m})$ เมื่อ m เป็นจำนวนเต็มลบ และ $m \equiv 1 \pmod 4$						←	—	→				
4. ค้นหาระบบส่วนตกค้างบริบูรณ์ ใน $\mathbb{Z}(\sqrt{m})$ เมื่อ m เป็นจำนวนเต็มลบ และ $m \equiv 1 \pmod 4$								←	→			
5. สรุปผลการศึกษาวิจัยและส่งผลงานวิจัยไปยังวารสารวิชาการ										←	→	
6. นำเสนอผลงานในงานประชุมวิชาการทางด้านคณิตศาสตร์หรือเผยแพร่ผลงานวิจัยทางเว็ปไซต์ของมหาวิทยาลัย												← →

14. ผลการวิจัย

รายละเอียดในภาคผนวก

15. ประโยชน์ที่ได้รับ

15.1 ผลงานวิจัยเกี่ยวกับระบบส่วนตกค้างบริบูรณ์ในสนามกำลังสองเชิงจินตภาพ

15.2 นำเสนอผลงานวิจัยในการประชุมวิชาการทางคณิตศาสตร์เพื่อเผยแพร่ผลงานและเกียรติคุณแก่มหาวิทยาลัยและหน่วยงานที่เกี่ยวข้อง

15.3 ผลงานวิจัยได้รับการตีพิมพ์ในวารสารทางคณิตศาสตร์เพื่อเผยแผ่ความรู้ให้เกิดประโยชน์ต่อการศึกษา การวิจัย และการพัฒนาประเทศ

16. งบประมาณของโครงการวิจัย

รายการ	จำนวนเงิน
1. ค่าตอบแทน	
1.1 ค่าตอบแทนผู้วิจัย	2,500 บาท
1.2 ค่าตอบแทนที่ปรึกษาโครงการ	2,500 บาท
1.3 ค่าตอบแทนผู้ร่วมวิจัย	2,500 บาท
2. ค่าใช้สอย	
2.1 ค่าลงทะเบียนเข้าร่วมประชุมวิชาการ	500 บาท
2.2 ค่าเช่าที่พักระหว่างเข้าร่วมประชุมวิชาการ	1,000 บาท
2.3 ค่าพาหนะเดินทางเข้าร่วมประชุมวิชาการ	1,000 บาท
3. ค่าวัสดุ	
3.1 ค่าหนังสือ วารสารและตำรา	1,000 บาท
3.2 ค่ากระดาษ	1,000 บาท
3.3 ค่าถ่ายเอกสารและเข้าเล่ม	1,000 บาท
3.4 ค่าวัสดุสำนักงาน	1,000 บาท
4. ค่าสาธารณูปโภค	1,000 บาท
รวมงบประมาณที่เสนอขอ	15,000 บาท

หมายเหตุ ขอถัวเฉลี่ยจ่ายทุกรายการ

ภาคผนวก

Explicit complete residue systems in a general quadratic field

Suton Tadee[1]*, Vichian Laohakosol[2]† and Santad Damkaew[3]
[1]Department of Mathematics, Faculty of Science and Technology,
Thepsatri Rajabhat University, Lopburi 15000, Thailand
[2]Department of Mathematics, Faculty of Science, Kasetsart University, Bangkok 10900, Thailand
[3]Department of Mathematics and Computer Science, Chulalongkorn University,
Bangkok 10330, Thailand
[1]suton.t@tru.ac.th, [2]fscivil@ku.ac.th, [3]s.damkaew@hotmail.co.th

Abstract

Bergum explicitly determined three representations for a complete residue system in the quadratic field $\mathbb{Q}(\sqrt{-3})$ extending two earlier results in $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$. Among these three representations, the first is simplest to derive, while the third is minimal in the sense that the sum of their absolute values is minimal. Here, we extend these results by deriving explicit representations for a complete residue system in any general quadratic field. The first representation uses lattice points in a rectangle in the first quadrant of an appropriate plane, while the second representation uses lattice points in a parallelogram, and the third representation uses lattice points in a hexagon and possesses a minimality property for imaginary quadratic fields.

2010 Mathematics Subject Classification: 11A07, 11R04
Key words and phrases: quadratic field, complete residue system, lattice point

1 Introduction

The problem of explicitly determining complete residue systems in a general number field is non-trivial, useful and interesting. Apart from the simplest case of the rational number field [6, p. 57], not much is known for other algebraic number fields. Regarding the quadratic field, Jordan and Potratz [4] treated those in the Gaussian field $\mathbb{Q}(\sqrt{-1})$, Potratz [5] considered those in $\mathbb{Q}(\sqrt{-2})$, and Bergum [1] worked out those in $\mathbb{Q}(\sqrt{-3})$. The objective of this work is to extend these results by determining three representations of a complete residue system in any general quadratic field $\mathbb{Q}(\sqrt{m})$.

Throughout the entire paper, the following notation and terminology will be kept fixed.

1) m is a squarefree integer, $m \notin \{0, 1\}$;

*Supported by the Faculty of Science and Technology, Thepsatri Rajabhat University.
†Supported by the Center for Advanced Studies in Industrial Technology and the Faculty of Science, Kasetsart University.

2) $\sigma_m := \begin{cases} -\frac{1}{2} + \frac{\sqrt{m}}{2} & \text{if } m \equiv 1 \pmod 4 \\ \sqrt{m} & \text{if } m \not\equiv 1 \pmod 4; \end{cases}$

3) $\mathbb{Z}[\sigma_m] = \{a + b\sigma_m : \ a, b \in \mathbb{Z}\}$ is the ring of integers of $\mathbb{Q}(\sqrt{m})$;

4) $\gamma = a + b\sigma_m \in \mathbb{Z}[\sigma_m] \setminus \{0\}$ is a fixed element with (γ) being its principal ideal;

5) $N(\gamma) := \gamma\overline{\gamma} = \begin{cases} a^2 - ab + b^2(1-m)/4 & \text{if } m \equiv 1 \pmod 4 \\ a^2 - mb^2 & \text{if } m \not\equiv 1 \pmod 4 \end{cases}$
denotes the norm of γ;

6) by lattice points, we refer to the elements of $\mathbb{Z}[\sigma_m]$;

7) by a complete residue system modulo (γ) (or modulo γ), [3, Chapter IX], abbreviated by $CRS(\gamma)$, we mean a set of $|N(\gamma)|$ elements $\{\xi_1, \xi_2, \ldots, \xi_{|N(\gamma)|}\}$ such that
i) $\xi_i \not\equiv \xi_j \pmod \gamma$ for all $i, j \in \{1, 2, \ldots, |N(\gamma)|\}$ with $i \neq j$, and
ii) for each $\alpha \in \mathbb{Z}[\sigma_m]$, there is a unique $\xi_i \in CRS(\gamma)$ such that $\alpha \equiv \xi_i \pmod \gamma$.

Note that, in case $m \equiv 1 \pmod 4$, we have

$$\sigma_m^2 = -\sigma_m + \frac{m-1}{4}. \tag{1.1}$$

Our starting point is the following lemma which gives the least natural number divisible by γ; here and throughout divisibility refers to that in the ring $\mathbb{Z}[\sigma_m]$.

Lemma 1.1. *Let $\gamma = a + b\sigma_m \in \mathbb{Z}[\sigma_m] \setminus \{0\}$. If $d = \gcd(a, b) \in \mathbb{N}$ so that*

$$\gamma = d\mu, \quad \textit{where } \mu := a_1 + b_1\sigma_m \in \mathbb{Z}[\sigma_m], \ \gcd(a_1, b_1) = 1,$$

then $d\,|N(\mu)|$ is the least natural number divisible by γ.

Proof. Let $c \in \mathbb{N}$ be divisible by γ. Then there exists $\alpha = p + q\sigma_m \in \mathbb{Z}[\sigma_m]$ such that

$$c = \gamma\alpha = d(a_1 + b_1\sigma_m)(p + q\sigma_m). \tag{1.2}$$

Consider four possible cases depending on b_1 and q.

1. If $b_1 = 0$ and $q = 0$, since $\gcd(a_1, b_1) = 1$, we have $a_1 = \pm 1$, and (1.2) gives $c = \pm dp$, yielding $|c| = d\,|p| \geq d\,|N(\mu)|$.

2. If $b_1 = 0$ and $q \neq 0$, since $\gcd(a_1, b_1) = 1$, we have $a_1 = \pm 1$, and (1.2) gives $c = \pm(dp + dq\sigma_m)$, which is impossible because $q \neq 0$.

3. If $b_1 \neq 0$ and $q = 0$, from (1.2), we have $c = dpa_1 + dpb_1\sigma_m$, which implies that $p = 0$, yielding $c = 0$, a contradiction.

4. If $b_1 \neq 0$ and $q \neq 0$, there are two possible subcases depending on the value of m mod 4. If $m \equiv 1 \pmod 4$, using (1.1) and (1.2), we have

$$c = d\left\{a_1 p - \left(\frac{1-m}{4}\right) b_1 q\right\} + d(a_1 q + b_1 p - b_1 q)\sigma_m \tag{1.3}$$

implying that

$$a_1 q + b_1 p - b_1 q = 0, \quad \text{i.e.,} \quad a_1 q = b_1 (q - p). \tag{1.4}$$

Thus, $b_1 | q$, say, $q = b_1 l$, for some $l \in \mathbb{Z}$. Substituting into (1.4), we get $p = l(b_1 - a_1)$. Putting back into (1.3), we have $c = -ld\left(a_1^2 - a_1 b_1 + (1-m)b_1^2/4\right)$, and so $c = |-l|\, d\, |N(\mu)| \geq d\, |N(\mu)|$.

If $m \not\equiv 1 \pmod 4$, using (1.2), we have

$$c = d(a_1 p + b_1 q m) + d(a_1 q + b_1 p)\sqrt{m}. \tag{1.5}$$

implying that

$$a_1 q + b_1 p = 0, \quad \text{i.e.,} \quad a_1 q = b_1 (-p). \tag{1.6}$$

Thus, $b_1 | q$, say, $q = b_1 l$, for some $l \in \mathbb{Z}$. Substituting into (1.6), we get $p = -a_1 l$. Putting back into (1.5), we have $c = -dl\left(a_1^2 - m b_1^2\right)$, and so $c = |-l|\, d\, |N(\mu)| \geq d\, |N(\mu)|$.

□

2 Representation I

Our first representation consists of lattice points in a rectangle in the first quadrant of the plane $\mathbb{R} \times \mathbb{R}\sqrt{m} = \{x + y\sqrt{m} : x, y \in \mathbb{R}\}$.

Theorem 2.1. *I. Keeping the notation of Lemma 1.1, consider the case* $m \equiv 1 \pmod 4$.
A) If d *is even, let*

$$T_1 := \left\{x + y\sqrt{m} : x, y \in \mathbb{Z},\ 0 \leq x \leq d\,|N(\mu)| - 1,\ 0 \leq y \leq \frac{d-2}{2}\right\}$$

$$T_2 := \left\{\left(x + \frac{1}{2}\right) + \left(y + \frac{1}{2}\right)\sqrt{m} : x, y \in \mathbb{Z},\ 0 \leq x \leq d\,|N(\mu)| - 1,\ 0 \leq y \leq \frac{d-2}{2}\right\},$$

then $T = T_1 \cup T_2$ *is a* $CRS(\gamma)$.
B) If d *is odd, let*

$$T_1; = \left\{x + y\sqrt{m} :\ x, y \in \mathbb{Z},\ 0 \leq x \leq d\,|N(\mu)| - 1,\ 0 \leq y \leq \frac{d-1}{2}\right\}$$

$$T_2 := \left\{\left(x + \frac{1}{2}\right) + \left(y + \frac{1}{2}\right)\sqrt{m} :\ x, y \in \mathbb{Z},\ 0 \leq x \leq d\,|N(\mu)| - 1,\ 0 \leq y \leq \frac{d-3}{2}\right\},$$

then $T = T_1 \cup T_2$ *is a* $CRS(\gamma)$.
II. For the case $m \not\equiv 1 \pmod 4$, *the set*

$$T := \left\{x + y\sqrt{m} : x, y \in \mathbb{Z},\ 0 \le x \le d\,|N(\mu)| - 1,\ 0 \le y \le d - 1\right\},$$

is a $CRS(\gamma)$.

Proof. I. Let $m \equiv 1 \pmod 4$.
A) When d is even, we first show that the elements in T are distinct modulo γ. Let $\alpha_1, \alpha_2 \in T$ be such that $\alpha_1 \equiv \alpha_2 \pmod\gamma$. Then there exists $\delta = a_2 + b_2\sigma_m \in \mathbb{Z}[\sigma_m]$ such that

$$\alpha_1 - \alpha_2 = \gamma\delta = d(a_1 + b_1\sigma_m)(a_2 + b_2\sigma_m). \tag{2.1}$$

From (1.1) and (2.1), we have

$$\alpha_1 - \alpha_2 = \frac{d}{2}\left\{\left(2a_1a_2 - a_1b_2 - a_2b_1 + \left(\frac{1+m}{2}\right)b_1b_2\right) + (a_1b_2 + a_2b_1 - b_1b_2)\sqrt{m}\right\}. \tag{2.2}$$

There are three possibilities.

Possibility 1: Both α_1 *and* α_2 *are elements of* T_1. Then they must be of the form

$$\alpha_i = x_i + y_i\sqrt{m} \qquad (i = 1, 2), \tag{2.3}$$

where $x_i, y_i \in \mathbb{Z}$, $0 \le x_i \le d\,|N(\mu)| - 1$ and $0 \le y_i \le \frac{d-2}{2}$. Substituting into (2.2) and equating the irrational parts, we get $y_1 - y_2 = \frac{d}{2}(a_1b_2 + a_2b_1 - b_1b_2)$, showing that $\frac{d}{2} \mid (y_1 - y_2)$. Since $0 \le y_i \le \frac{d-2}{2}$, we have $0 \le |y_1 - y_2| \le \frac{d-2}{2} < \frac{d}{2}$, which together with the last divisibility imply that $y_1 = y_2$. Thus, (2.1)-(2.3) yield $\gamma|(x_1 - x_2)$. Since $0 \le x_i \le d\,|N(\mu)| - 1$, we have $0 \le |x_1 - x_2| \le d\,|N(\mu)| - 1 < d\,|N(\mu)|$. Invoking upon Lemma 1.1, we deduce that $x_1 = x_2$, and so $\alpha_1 = \alpha_2$.

Possibility 2: Both α_1 *and* α_2 *are elements of* T_2. Then

$$\alpha_i = \left(x_i + \frac{1}{2}\right) + \left(y_i + \frac{1}{2}\right)\sqrt{m} \qquad (i = 1, 2), \tag{2.4}$$

where $x_i, y_i \in \mathbb{Z}$, $0 \le x_i \le d\,|N(\mu)| - 1$ and $0 \le y_i \le \frac{d-2}{2}$. Proceeding exactly as in Possibility 1, we deduce that $\alpha_1 = \alpha_2$.

Possibility 3: One of the α_i, *say,* $\alpha_1 \in T_1$, *while* $\alpha_2 \in T_2$. Then

$$\alpha_1 = x_1 + y_1\sqrt{m},\ \ \alpha_2 = \left(x_2 + \frac{1}{2}\right) + \left(y_2 + \frac{1}{2}\right)\sqrt{m},$$

where $x_i, y_i \in \mathbb{Z}$, $0 \le x_i \le d\,|N(\mu)| - 1$, $0 \le y_i \le \frac{d-2}{2}$ $(i = 1, 2)$. Substituting into (2.2) and equating the irrational parts, we get $y_1 - y_2 - 1/2 = d\,(a_1b_2 + a_2b_1 - b_1b_2)\,/2$, which is a contradiction because the right-hand side is an integer while the left-hand side is not.

There remains to show that each element $\alpha = x + y\sigma_m \in \mathbb{Z}[\sigma_m]$ is congruent mod γ to an element of T_1 or T_2. By the Euclidean algorithm, there exist $q_1, r_1 \in \mathbb{Z}$ such that

$$y = dq_1 + r_1 \qquad (0 \le r_1 < d).$$

Since $d = \gcd(a, b)$, there exist $u, v \in \mathbb{Z}$ such that $au + bv = dq_1$. These last two relations give

$$y = au + bv + r_1. \tag{2.5}$$

To finish the proof of this part, we treat two possible cases depending on the parity of r_1.

Case 1: r_1 is even, say, $r_1 = 2n_1$ ($n_1 \in \mathbb{N}_0$). The next step involves a clever choosing of elements. By the Euclidean algorithm, there exist $q_2, n_2 \in \mathbb{Z}$ such that

$$x - n_1 - av - au + (1 - m)\, bu/4 = d\,|N(\mu)|\, q_2 + n_2, \quad 0 \le n_2 < d\,|N(\mu)|\,,$$

and so

$$x = d\,|N(\mu)|\, q_2 + n_2 + n_1 + av + au - (1 - m)\, bu/4. \tag{2.6}$$

Using (2.5)-(2.6), we have

$$\begin{aligned} \alpha = x + y\sigma_m &= d\,|N(\mu)|\, q_2 + n_2 + n_1 + av + au - (1 - m)\, bu/4 + (au + bv + r_1)\sigma_m \\ &= d\,|N(\mu)|\, q_2 + (v + u(1 + \sigma_m))\gamma + n_2 + n_1\sqrt{m}. \end{aligned}$$

Since $d\,|N(\mu)| \equiv 0 \pmod{\gamma}$, we have

$$\alpha \equiv n_2 + n_1\sqrt{m} \pmod{\gamma}. \tag{2.7}$$

Since $0 \le n_2 < d\,|N(\mu)|$, $0 \le r_1 = 2n_1 < d$, and d is even, we have $0 \le n_2 \le d\,|N(\mu)| - 1$, $0 \le n_1 \le (d-2)/2$. Thus, modulo γ, we have $\alpha \equiv n_2 + n_1\sqrt{m} \in T_1$.

Case 2: r_1 is odd, say, $r_1 = 2n_1 + 1$ ($n_1 \in \mathbb{N}_0$). Proceeding in a manner similar to the previous case, there exist $q_2, n_2 \in \mathbb{Z}$ such that

$$x - n_1 - 1 - av - au + (1 - m)\, bu/4 = d\,|N(\mu)|\, q_2 + n_2 \qquad (0 \le n_2 < d\,|N(\mu)|).$$

Then

$$\begin{aligned} \alpha = x + y\sigma_m &= d\,|N(\mu)|\, q_2 + n_2 + n_1 + 1 + av + au - (1 - m)\, bu/4 + (au + bv + r_1)\sigma_m \\ &= d\,|N(\mu)|\, q_2 + (v + u(1 + \sigma_m))\gamma + n_2 + 1/2 + (n_1 + 1/2)\sqrt{m} \\ &\equiv (n_2 + 1/2) + (n_1 + 1/2)\sqrt{m} \pmod{\gamma}. \end{aligned}$$

Since $0 \le n_2 < d\,|N(\mu)|$ and $0 \le n_1 = \frac{r_1 - 1}{2} \le \frac{d-2}{2}$, we see that α is congruent mod γ to an element in T_2.

B) We proceed now to the case where d is odd. To show that the elements in T are distinct mod γ, let $\alpha_1, \alpha_2 \in T$ be such that $\alpha_1 \equiv \alpha_2 \pmod{\gamma}$. Then there exists $\delta = a_2 + b_2\sigma_m \in \mathbb{Z}[\sigma_m]$ such that

$$\alpha_1 - \alpha_2 = \gamma\delta = d(a_1 + b_1\sigma_m)(a_2 + b_2\sigma_m). \tag{2.8}$$

There are three possibilities.

Possibility 1: Both α_1 and α_2 are elements of T_1. Then

$$\alpha_i = x_i + y_i\sqrt{m} \qquad (i = 1, 2),$$

where $x_i, y_i \in \mathbb{Z}$, $0 \le x_i \le d\,|N(\mu)| - 1$ and $0 \le y_i \le \frac{d-1}{2}$. Substituting into (2.8) and multiplying by 2, we have

$$\begin{aligned} &2(x_1 - x_2) + 2(y_1 - y_2)\sqrt{m} \\ &= d\left(\left(2a_1a_2 + \left(\frac{m+1}{2}\right)b_1b_2 - a_1b_2 - b_1a_2\right) + (a_1b_2 + b_1a_2 - b_1b_2)\sqrt{m}\right) \end{aligned}$$

Equating the irrational part, we get $2(y_1 - y_2) = d(a_1b_2 + b_1a_2 - b_1b_2)$, which shows that $d \mid 2(y_1 - y_2)$. Since $0 \le y_i \le (d-1)/2$ $(i = 1, 2)$, we deduce at once that $y_1 = y_2$, and consequently, $x_1 \equiv x_2 \pmod{\gamma}$. Since $0 \le x_i \le d\,|N(\mu)| - 1$ $(i = 1, 2)$, Lemma 1.1 shows immediately that $x_1 = x_2$, and so $\alpha_1 = \alpha_2$.

Possibility 2: Both α_1 and α_2 are elements in T_2. Then

$$\alpha_i = \left(x_i + \frac{1}{2}\right) + \left(y_i + \frac{1}{2}\right)\sqrt{m} \qquad (i = 1, 2),$$

where $x_i, y_i \in \mathbb{Z}, 0 \le x_i \le d\,|N(\mu)| - 1$ and $0 \le y_i \le \frac{d-3}{2}$. Proceeding exactly as in Possibility 1, we deduce that $\alpha_1 = \alpha_2$.

Possibility 3: One of the α_i, say, $\alpha_1 \in T_1$, while $\alpha_2 \in T_2$. Then

$$\alpha_1 = x_1 + y_1\sqrt{m}, \quad \alpha_2 = (x_2 + \frac{1}{2}) + \left(y_2 + \frac{1}{2}\right)\sqrt{m},$$

where $x_i, y_i \in \mathbb{Z}$, $0 \le x_i \le d\,|N(\mu)| - 1$ $(i = 1, 2)$, $0 \le y_1 \le \frac{d-1}{2}$ and $0 \le y_2 \le \frac{d-3}{2}$. Substituting into (2.8) and multiplying by 2, we have

$$\begin{aligned} &(2x_1 - 2x_2 - 1) + (2y_1 - 2y_2 - 1)\sqrt{m} \\ &= d\left\{\left(2a_1a_2 + \frac{m+1}{2}b_1b_2 - a_1b_2 - b_1a_2\right) + (a_1b_2 + b_1a_2 - b_1b_2)\sqrt{m}\right\}. \end{aligned}$$

Equating the irrational part, we get $d \mid (2y_1 - 2y_2 - 1)$. Since $0 \le y_1 \le (d-1)/2$ and $0 \le y_2 \le (d-3)/2$, we deduce that $2y_1 = 2y_2 + 1$, which is a contradiction because the left-hand side is even, while the right-hand side is odd.

There remains to show that each element $\alpha = x + y\sigma_m \in \mathbb{Z}[\sigma_m]$ is congruent mod γ to an element of T. By the Euclidean algorithm, there exist $q_1, r_1 \in \mathbb{Z}$ such that $y = dq_1 + r_1$, $0 \le r_1 < d$. Since $d = \gcd(a, b)$, there exist $u, v \in \mathbb{Z}$ such that $au + bv = dq_1$, and so $y = au + bv + r_1$. We treat three possible cases.

Case 1: r_1 is even, say $r_1 = 2n_1$ $(n_1 \in \mathbb{N}_0)$. Then there exist $q_2, n_2 \in \mathbb{Z}$ such that

$$x - n_1 - av - au + (1 - m)\,bu/4 = d\,|N(\mu)|\,q_2 + n_2, \quad 0 \le n_2 < d\,|N(\mu)|\,,$$

and so

$$\begin{aligned}\alpha &= x + y\sigma_m \\ &= d\,|N(\mu)|\,q_2 + n_2 + n_1 + av + au - \left(\frac{1-m}{4}\right)bu + (au + bv + r_1)\left(\frac{-1}{2} + \frac{\sqrt{m}}{2}\right) \\ &= d\,|N(\mu)|\,q_2 + (v + u(1+\sigma_m))\gamma + n_2 + n_1\sqrt{m} \\ &\equiv n_2 + n_1\sqrt{m} \pmod{\gamma}.\end{aligned}$$

Since $0 \le n_2 < d\,|N(\mu)|$, $0 \le n_1 = r_1/2 \le (d-1)/2$, we have $n_2 + n_1\sqrt{m} \in T_1$.

Case 2: r_1 is odd, say, $r_1 = 2n_1 + 1$ ($n_1 \in \mathbb{N}_0$). Then there exist $q_2, n_2 \in \mathbb{Z}$ such that

$$x - n_1 - 1 - av - au + (1-m)\,bu/4 = d\,|N(\mu)|\,q_2 + n_2,\ 0 \le n_2 < d\,|N(\mu)|.$$

Then

$$\begin{aligned}\alpha &= x + y\sigma_m \\ &= d\,|N(\mu)|\,q_2 + n_2 + n_1 + 1 + av + au - \left(\frac{1-m}{4}\right)bu + (au + bv + r_1)\left(\frac{-1}{2} + \frac{\sqrt{m}}{2}\right) \\ &= d\,|N(\mu)|\,q_2 + (v + u(1+\sigma_m))\gamma + n_2 + 1/2 + (n_1 + 1/2)\,\sqrt{m} \\ &\equiv (n_2 + 1/2) + (n_1 + 1/2)\,\sqrt{m} \pmod{\gamma}.\end{aligned}$$

Since $0 \le n_2 < d\,|N(\mu)|$, $0 \le n_1 = (r_1 - 1)/2 \le (d-3)/2$ (because d is odd), we have $(n_2 + 1/2) + (n_1 + 1/2)\,\sqrt{m} \in T_2$.

II. Let $m \not\equiv 1 \pmod 4$. To show that the elements in T are distinct mod γ, let

$$\alpha_i = x_i + y_i\sqrt{m} \in T \qquad (i = 1, 2), \tag{2.9}$$

where $x_i, y_i \in \mathbb{Z}$, $0 \le x_i \le d\,|N(\mu)| - 1$ and $0 \le y_i \le d - 1$, be such that $\alpha_1 \equiv \alpha_2 \pmod{\gamma}$. Then there exists $\delta = a_2 + b_2\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ such that $\alpha_1 - \alpha_2 = \gamma\delta$, and so

$$(x_1 - x_2) + (y_1 - y_2)\sqrt{m} = d\,(a_1a_2 + b_1b_2m) + d\,(a_1b_2 + a_2b_1)\,\sqrt{m}. \tag{2.10}$$

Substituting into (2.10) and equating the irrational parts, we get $y_1 - y_2 = d(a_1b_2 + a_2b_1)$, showing that $d \mid (y_1 - y_2)$. Since $0 \le y_i \le d - 1$, we have $0 \le |y_1 - y_2| \le d - 1 < d$, which together with the last divisibility imply that $y_1 = y_2$. Thus, (2.10) yields $\gamma|(x_1 - x_2)$. Since $0 \le x_i \le d\,|N(\mu)| - 1$, we have $0 \le |x_1 - x_2| \le d\,|N(\mu)| - 1 < d\,|N(\mu)|$. Invoking upon Lemma 1.1, we deduce that $x_1 = x_2$, and so $\alpha_1 = \alpha_2$.

Next, we show that each element $\alpha = x + y\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ is congruent mod γ to an element of T. By the Euclidean algorithm, there exist $q_1, r_1 \in \mathbb{Z}$ such that

$$y = dq_1 + r_1 \qquad (0 \le r_1 < d).$$

Since $d = \gcd(a, b)$, there exist $u, v \in \mathbb{Z}$ such that $au + bv = dq_1$. These last two relations give

$$y = au + bv + r_1. \tag{2.11}$$

By the Euclidean algorithm, there exist $q_2, r_2 \in \mathbb{Z}$ such that

$$x - av - ubm = d\,|N(\mu)|\,q_2 + r_2, \quad 0 \le r_2 < d\,|N(\mu)|\,,$$

and so

$$x = d\,|N(\mu)|\,q_2 + r_2 + av + ubm. \tag{2.12}$$

Using (2.11)-(2.12), we have

$$\begin{aligned}\alpha = x + y\sqrt{m} &= d\,|N(\mu)|\,q_2 + r_2 + av + ubm + (au + bv + r_1)\sqrt{m} \\ &= d\,|N(\mu)|\,q_2 + av + ubm + au\sqrt{m} + bv\sqrt{m} + r_2 + r_1\sqrt{m} \\ &= d\,|N(\mu)|\,q_2 + (v + u\sqrt{m})(a + b\sqrt{m}) + r_2 + r_1\sqrt{m} \\ &= d\,|N(\mu)|\,q_2 + (v + u\sqrt{m})\gamma + r_2 + r_1\sqrt{m}.\end{aligned}$$

From Lemma 1.1, we have

$$\alpha \equiv r_2 + r_1\sqrt{m} \pmod{\gamma}. \tag{2.13}$$

Since $0 \le r_2 < d\,|N(\mu)|$ and $0 \le r_1 < d$, we have $0 \le r_2 \le d\,|N(\mu)| - 1$, $0 \le r_1 \le d - 1$. Thus, modulo γ, we have $\alpha \equiv r_2 + r_1\sqrt{m} \in T$. □

3 Representation II

Our second representation makes use of lattice points in a parallelogram. We begin with a simple lemma.

Lemma 3.1. *For any $\alpha_1 = a_1 + b_1\sigma_m \in \mathbb{Z}[\sigma_m]$, we have*

$$\frac{\alpha_1}{\gamma} = (r_1 + s_1\sigma_m) + (R_1 + S_1\sigma_m), \tag{3.1}$$

where $r_1, s_1 \in \mathbb{Z}$, and $R_1, S_1 \in \mathbb{Q} \cap [-1/2, 1/2)$.

Proof. Multiplying $\alpha_1/\gamma = (a_1 + b_1\sigma_m)/(a + b\sigma_m)$ by the conjugate of the denominator, we get

$$\frac{\alpha_1}{\gamma} = \frac{a_1 + b_1\sigma_m}{a + b\sigma_m} = C_1 + D_1\sigma_m, \tag{3.2}$$

where

$$C_1 := \begin{cases} \left(a_1a - a_1b + \frac{1-m}{4}b_1b\right)/N(\gamma) & \text{if } m \equiv 1 \pmod 4 \\ (a_1a - b_1bm)/N(\gamma) & \text{if } m \not\equiv 1 \pmod 4 \end{cases}$$

and $D_1 := (b_1a - a_1b)/N(\gamma)$. The desired shape follows by taking

$$r_1 = \left\lfloor C_1 + \frac{1}{2} \right\rfloor, \; s_1 = \left\lfloor D_1 + \frac{1}{2} \right\rfloor, \; R_1 = C_1 - r_1, \; S_1 = D_1 - s_1.$$

□

Our second representation is given in

Theorem 3.2. *Let V_1 be the collection of lattice points inside the parallelogram $ABCD$ whose vertices are, respectively,*

$$A = \frac{\gamma}{2}(1+\sigma_m),\ B = \frac{\gamma}{2}(1-\sigma_m),\ C = \frac{\gamma}{2}(-1-\sigma_m),\ D = \frac{\gamma}{2}(-1+\sigma_m),$$

and let V_2 be the collection of the lattice points on the half-open line segments BC and CD excluding the points B and D, but possibly including the points C (if $C \in \mathbb{Z}[\sigma_m]$). Then $V = V_1 \cup V_2$ is a $CRS(\gamma)$.

Proof. From Lemma 3.1, we have $\alpha_1 \equiv (R_1 + S_1\sigma_m)\gamma \pmod{\gamma}$. The equations of the line segments AB, BC, CD and DA are, respectively,

$$\gamma\left(\frac{1}{2} + \frac{2t-1}{2}\sigma_m\right),\ \gamma\left(\frac{2t-1}{2} - \frac{\sigma_m}{2}\right),\ \gamma\left(-\frac{1}{2} - \frac{2t-1}{2}\sigma_m\right),\ \gamma\left(-\frac{2t-1}{2} + \frac{\sigma_m}{2}\right),$$

where $t \in \mathbb{R} \cap [0,1]$.

- If $-1/2 < R_1 < 1/2$ and $-1/2 < S_1 < 1/2$, then $(R_1 + S_1\sigma_m)\gamma$ lies inside the parallelogram $ABCD$, yielding $(R_1 + S_1\sigma_m)\gamma \in V_1$.
- If $R_1 = -1/2$, then $(R_1 + S_1\sigma_m)\gamma$ lies on $\overline{CD}$ (excluding the point D), yielding $(R_1 + S_1\sigma_m)\gamma \in V_2$.
- If $S_1 = -1/2$, then $(R_1 + S_1\sigma_m)\gamma$ lies on $\overline{BC}$ (excluding the point B), yielding $(R_1 + S_1\sigma_m)\gamma \in V_2$.

These three possibilities show that each element of $\mathbb{Z}[\sigma_m]$ is congruent to some element of V. There remains to show that the elements in V are incongruent mod γ. Note first that each element $\alpha_1 \in V = V_1 \cup V_2$ when represented under the form (3.1) of Lemma 3.1 always has $r_1 = s_1 = 0$ and so (3.1) reduces to $\alpha_1 = (R_1 + S_1\sigma_m)\gamma$. Thus, for any $\alpha_1, \alpha_2 \in V$ with $\alpha_1 \equiv \alpha_2 \pmod{\gamma}$, we have $\alpha_1 = \alpha_2 + \delta\gamma$, where $\delta \in \mathbb{Z}[\sigma_m]$ satisfies

$$\delta = (R_1 - R_2) + (S_1 - S_2)\sigma_m.$$

Since $-1/2 \le R_1, R_2, S_1, S_2 < 1/2$, and $\delta \in \mathbb{Z}[\sigma_m]$, we deduce that $\delta = 0$, yielding $\alpha_1 = \alpha_2$. □

As pointed out in [1], it is of interest to find out when the set V_2 in Theorem 3.2 is empty, which we solve in the next proposition.

Proposition 3.3. *Keeping the notation of Theorem 3.2, let $m \equiv 1 \pmod 4$.*
I. If $(1-m)/4$ is even, then the set V_2 is empty if and only if $N(\gamma)$ is not divisible by 2.
II. If $(1-m)/4$ is odd, then the set V_2 is empty if and only if γ is not divisible by 2.

Proof. I. Let $(1-m)/4$ be even. If V_2 is empty, assuming $N(\gamma)$ is divisible by 2, we see that

$$N(\gamma) = a^2 - ab + \left(\frac{1-m}{4}\right) b^2 = a(a-b) + \left(\frac{1-m}{4}\right) b^2$$

is even, showing that either a is even, or a and b are both odd. If a is even, since

$$C = -\frac{a}{2} - \frac{b}{2}\left(\frac{m-1}{4}\right) - \frac{a}{2}\sigma_m \in \mathbb{Z}[\sigma_m],$$

the vertex C is a point of V_2. If a and b are both odd, choosing $t = 1/2$ in the parametric representation of the line BC given in Theorem 3.2, we see that there is a vertex in V_2, viz.,

$$\gamma\left(-\frac{\sigma_m}{2}\right) = -\frac{b}{2}\left(\frac{m-1}{4}\right) + \left(\frac{-a+b}{2}\right)\sigma_m \in \mathbb{Z}[\sigma_m].$$

In either case, the set V_2 is non-empty, which is a contradiction.

On the other hand, if $N(\gamma)$ is not divisible by 2, assume that $V_2 \neq \phi$. For $\alpha_1 = a_1 + b_1\sigma_m \in V_2$, we see that α_1 lies either on $\overline{BC}$ or on $\overline{CD}$. If α_1 lies on $\overline{BC}$, then from (3.2), we have $\frac{b_1 a - a_1 b}{N(\gamma)} = -\frac{1}{2}$, and so $N(\gamma)$ is divisible by 2, a contradiction. If α_1 lies on $\overline{CD}$, then from (3.2), we have $\frac{1}{N(\gamma)}\left(a_1 a - a_1 b + \frac{1-m}{4} b_1 b\right) = -\frac{1}{2}$, showing that $N(\gamma)$ is divisible by 2, again a contradiction.

II. Let $(1-m)/4$ be odd. If V_2 is empty, assuming $2|\gamma$, we see that the point C is

$$\frac{\gamma}{2}(-1-\sigma_m) = -\frac{a}{2} - \frac{b}{2}\left(\frac{m-1}{4}\right) - \frac{a}{2}\sigma_m \in \mathbb{Z}\left[\sigma_m\right],$$

and so $C \in V_2$, contradicting the emptiness of V_2.

On the other hand, assume now that $2 \nmid \gamma$. If V_2 is non-empty, then let $\alpha_1 = a_1 + b_1\sigma_m \in V_2$, so that α_1 lies either on $\overline{BC}$ or on $\overline{CD}$. We pause to prove an auxiliary result.

Claim. The number $N(\gamma)$ is divisible by 2 if and only if $2|\gamma$.

Proof of Claim. We have

$$N(\gamma) = a^2 - ab + \frac{1-m}{4} b^2 = (a-b)^2 + ab + \left(\frac{1-m}{4} - 1\right) b^2.$$

If $N(\gamma)$ is divisible by 2, since $(1-m)/4$ is odd, then $a-b$ and ab are of the same parity. If $a-b$ is odd, then a and b have opposite parity, yielding ab even, a contradiction. If $a-b$ is even, then a and b have the same parity. Since ab is even, both a and b are even, implying that γ is divisible by 2. The other implication is trivial, and the claim is proved.

Returning now to the proof of part II, if α_1 lies on $\overline{BC}$, from (3.2), we have $2\left(b_1 a - a_1 b\right) = -N(\gamma)$, while if α_1 lies on $\overline{CD}$, from (3.2), we have

$$2\left(a_1 a - a_1 b + \frac{1-m}{4} b_1 b\right) = -N(\gamma).$$

In either case $N(\gamma)$ is divisible by 2. Using the claim, we deduce that γ is divisible by 2, which is a contradiction. □

Proposition 3.3 gives the following generalization of Bergum's result [1].

Theorem 3.4. *Let the notation be as in Theorem 3.2. Then $V_2 = \phi$ if and only if $N(\gamma)$ is not divisible by 2 .*

Proof. The case $m \equiv 1 \pmod 4$ has already been proved in Proposition 3.3. Consider now $m \not\equiv 1 \pmod 4$.

If V_2 is empty, assuming $N(\gamma)$ is divisible by 2, we see that

$$N(\gamma) = a^2 - mb^2 \tag{3.3}$$

is even. We treat two possibilities cases depending on the parity of m.

Possibility 1: m is even. From (3.3), a is also even. Choosing $t = 1/2$ in the parametric representation of the line BC given in Theorem 3.2, we see that there is a vertex in V_2, viz.,

$$\gamma\left(-\frac{\sqrt{m}}{2}\right) = -\frac{bm}{2} - \frac{a\sqrt{m}}{2} \in \mathbb{Z}[\sqrt{m}], \tag{3.4}$$

showing that the set V_2 is non-empty, which is a contradiction.

Possibility 2: m is odd, say $m = 2k + 1$ ($k \in \mathbb{Z}$). Substituting into (3.3), we get

$$N(\gamma) = (a - b)(a + b) - 2kb^2. \tag{3.5}$$

Since $N(\gamma)$ is even, either a and b are both even, or a and b are both odd. If a and b are both even, the relation (3.4) yields $\gamma\,(-\sqrt{m}/2) \in V_2$. If a and b are both odd, since

$$C = \frac{\gamma}{2}(-1 - \sqrt{m}) = -\frac{a + bm}{2} - \frac{a + b}{2}\sqrt{m} \in \mathbb{Z}[\sqrt{m}],$$

the vertex C is a point of V_2. In either case, the set V_2 is non-empty, which is a contradiction.

To establish the other implication, assume that $N(\gamma)$ is not divisible by 2. If $V_2 \neq \phi$, then for $\alpha_1 = a_1 + b_1\sqrt{m} \in V_2$, we see that α_1 lies either on $\overline{BC}$ or on $\overline{CD}$. If α_1 lies on $\overline{BC}$, then from (3.2), we have

$$\frac{ab_1 - a_1 b}{N(\gamma)} = -\frac{1}{2},$$

and so $N(\gamma)$ is divisible by 2, a contradiction. If α_1 lies on $\overline{CD}$, then from (3.2), we have

$$\frac{a_1 a - b_1 bm}{N(\gamma)} = -\frac{1}{2},$$

showing that $N(\gamma)$ is divisible by 2, again a contradiction. □

4 Representation III

Our last representation makes use of lattice points in a hexagon. Since this representation is so constructed to be minimal (in the sense that the sum of their absolute values is minimal), we need to adjust the parameters in Lemma 3.1 appropriately using the following claim.

Lemma 4.1. *For any $\alpha_1 = a_1 + b_1\sigma_m \in \mathbb{Z}[\sigma_m]$, there are rational integers r, s and rational numbers R, S such that*

$$\frac{\alpha_1}{\gamma} = (r + s\sigma_m) + (R + S\sigma_m), \tag{4.1}$$

where

$$-1 \le 2R - S < 1 \tag{4.2}$$

$$-\frac{|m|+1}{4} \le R + \left(\frac{|m|-1}{2}\right) S < \frac{|m|+1}{4} \tag{4.3}$$

$$-\frac{|m|+1}{4} \le \left(\frac{|m|+1}{2}\right) S - R < \frac{|m|+1}{4}. \tag{4.4}$$

(For convenience, a number written under the form (4.1) subject to (4.2)–(4.4) is said to be in a *standard form*).

Proof. By Lemma 3.1, we have $\alpha_1/\gamma = (r_1 + s_1\sigma_m) + (R_1 + S_1\sigma_m)$, where $r_1, s_1 \in \mathbb{Z}$, and $R_1, S_1 \in \mathbb{Q} \cap [-1/2, 1/2)$. We treat four possible cases depending on the subdivision of the ranges of R_1 and S_1, namely,

i) $-1/2 \le R_1 \le 0,\ -1/2 \le S_1 \le 0,$

ii) $0 < R_1 < 1/2,\ 0 < S_1 < 1/2,$

iii) $-1/2 \le R_1 \le 0,\ 0 < S_1 < 1/2,$

iv) $0 < R_1 < 1/2,\ -1/2 \le S_1 \le 0.$

For the cases i) and ii), the lemma follows by taking $r = r_1,\ s = s_1,\ R = R_1$ and $S = S_1$. As for case iii), since

$$-\tfrac{1}{2} < R_1 + \left(\tfrac{|m|-1}{2}\right) S_1 < \tfrac{|m|-1}{4}\ ,\ -\tfrac{3}{2} < 2R_1 - S_1 < 0\ ,\ 0 < \left(\tfrac{|m|+1}{2}\right) S_1 - R_1 < \tfrac{|m|+3}{4},$$

we split our consideration into eight possibilities.

iii.1) $-\frac{1}{2} < R_1 + \left(\frac{|m|-1}{2}\right) S_1 < \frac{|m|-3}{4},\ -\frac{3}{2} < 2R_1 - S_1 < -1$ and
$0 < \left(\frac{|m|+1}{2}\right) S_1 - R_1 < \frac{|m|+1}{4}.$
The result follows by taking $r = r_1 - 1,\ s = s_1,\ R = R_1 + 1,\ S = S_1.$

iii.2) $-\frac{1}{2} < R_1 + \left(\frac{|m|-1}{2}\right) S_1 < \frac{|m|-3}{4},\ -\frac{3}{2} < 2R_1 - S_1 < -1$ and
$\frac{|m|+1}{4} \le \left(\frac{|m|+1}{2}\right) S_1 - R_1 < \frac{|m|+3}{4}.$
The result follows by taking $r = r_1 - 1,\ s = s_1,\ R = R_1 + 1,\ S = S_1.$

iii.3) $-\frac{1}{2} < R_1 + \left(\frac{|m|-1}{2}\right) S_1 < \frac{|m|-3}{4},\ -1 \le 2R_1 - S_1 < 0$ and
$0 < \left(\frac{|m|+1}{2}\right) S_1 - R_1 < \frac{|m|+1}{4}.$
The result follows by taking $r = r_1,\ s = s_1,\ R = R_1,\ S = S_1.$

iii.4) $-\frac{1}{2} < R_1 + \left(\frac{|m|-1}{2}\right) S_1 < \frac{|m|-3}{4}$, $-1 \leq 2R_1 - S_1 < 0$ and
$\frac{|m|+1}{4} \leq \left(\frac{|m|+1}{2}\right) S_1 - R_1 < \frac{|m|+3}{4}$.
These three sets of inequalities are self-contradictory, so this possibility is ruled out.

iii.5) $\frac{|m|-3}{4} \leq R_1 + \left(\frac{|m|-1}{2}\right) S_1 < \frac{|m|-1}{4}$, $-3/2 < 2R_1 - S_1 < -1$ and
$0 < \left(\frac{|m|+1}{2}\right) S_1 - R_1 < \frac{|m|+1}{4}$.
The inequalities are self-contradictory.

iii.6) $\frac{|m|-3}{4} \leq R_1 + \left(\frac{|m|-1}{2}\right) S_1 < \frac{|m|-1}{4}$, $-3/2 < 2R_1 - S_1 < -1$ and
$\frac{|m|+1}{4} \leq \left(\frac{|m|+1}{2}\right) S_1 - R_1 < \frac{|m|+3}{4}$.
The result follows by taking $r = r_1,\ s = s_1 + 1,\ R = R_1,\ S = S_1 - 1$.

iii.7) $\frac{|m|-3}{4} \leq R_1 + \left(\frac{|m|-1}{2}\right) S_1 < \frac{|m|-1}{4}$, $-1 \leq 2R_1 - S_1 < 0$ and
$0 < \left(\frac{|m|+1}{2}\right) S_1 - R_1 < \frac{|m|+1}{4}$.
The result follows by taking $r = r_1,\ s = s_1,\ R = R_1,\ S = S_1$.

iii.8) $\frac{|m|-3}{4} \leq R_1 + \left(\frac{|m|-1}{2}\right) S_1 < \frac{|m|-1}{4}$, $-1 \leq 2R_1 - S_1 < 0$ and
$\frac{|m|+1}{4} \leq \left(\frac{|m|+1}{2}\right) S_1 - R_1 < \frac{|m|+3}{4}$.
The result follows by taking $r = r_1,\ s = s_1 + 1,\ R = R_1,\ S = S_1 - 1$.

We next turn to case iv). Since

$$-\tfrac{|m|-1}{4} < R_1 + \left(\tfrac{|m|-1}{2}\right) S_1 < \tfrac{1}{2},\ 0 < 2R_1 - S_1 < \tfrac{3}{2},\ -\tfrac{|m|+3}{4} < \left(\tfrac{|m|+1}{2}\right) S_1 - R_1 < 0,$$

we again split our consideration into eight possibilities.

iv.1) $-\frac{|m|-1}{4} < R_1 + \left(\frac{|m|-1}{2}\right) S_1 < -\frac{|m|-3}{4}$, $0 < 2R_1 - S_1 < 1$ and
$-\frac{|m|+3}{4} < \left(\frac{|m|+1}{2}\right) S_1 - R_1 < -\frac{|m|+1}{4}$.
The result follows by taking $r = r_1,\ s = s_1 - 1,\ R = R_1,\ S = S_1 + 1$.

iv.2) $-\frac{|m|-1}{4} < R_1 + \left(\frac{|m|-1}{2}\right) S_1 < -\frac{|m|-3}{4}$, $0 < 2R_1 - S_1 < 1$ and
$-\frac{|m|+1}{4} \leq \left(\frac{|m|+1}{2}\right) S_1 - R_1 < 0$.
The result follows by taking $r = r_1,\ s = s_1,\ R = R_1,\ S = S_1$.

iv.3) $-\frac{|m|-1}{4} < R_1 + \left(\frac{|m|-1}{2}\right) S_1 < -\frac{|m|-3}{4}$, $1 \leq 2R_1 - S_1 < \frac{3}{2}$ and
$-\frac{|m|+3}{4} < \left(\frac{|m|+1}{2}\right) S_1 - R_1 < -\frac{|m|+1}{4}$.
The result follows by taking $r = r_1,\ s = s_1 - 1,\ R = R_1,\ S = S_1 + 1$.

iv.4) $-\frac{|m|-1}{4} < R_1 + \left(\frac{|m|-1}{2}\right) S_1 < -\frac{|m|-3}{4}$, $1 \leq 2R_1 - S_1 < \frac{3}{2}$ and
$-\frac{|m|+1}{4} \leq \left(\frac{|m|+1}{2}\right) S_1 - R_1 < 0$.
The inequalities are self-contradictory.

iv.5) $-\frac{|m|-3}{4} \le R_1 + \left(\frac{|m|-1}{2}\right) S_1 < \frac{1}{2}$, $0 < 2R_1 - S_1 < 1$ and
$-\frac{|m|+3}{4} < \left(\frac{|m|+1}{2}\right) S_1 - R_1 < -\frac{|m|+1}{4}$.
The inequalities are self-contradictory.

iv.6) $-\frac{|m|-3}{4} \le R_1 + \left(\frac{|m|-1}{2}\right) S_1 < \frac{1}{2}$, $0 < 2R_1 - S_1 < 1$ and
$-\frac{|m|+1}{4} \le \left(\frac{|m|+1}{2}\right) S_1 - R_1 < 0$.
The result follows by taking $r = r_1$, $s = s_1$, $R = R_1$, $S = S_1$.

iv.7) $-\frac{|m|-3}{4} \le R_1 + \left(\frac{|m|-1}{2}\right) S_1 < \frac{1}{2}$, $1 \le 2R_1 - S_1 < \frac{3}{2}$ and
$-\frac{|m|+3}{4} < \left(\frac{|m|+1}{2}\right) S_1 - R_1 < -\frac{|m|+1}{4}$.
The result follows by taking $r = r_1 + 1$, $s = s_1$, $R = R_1 - 1$, $S = S_1$.

iv.8) $-\frac{|m|-3}{4} \le R_1 + \left(\frac{|m|-1}{2}\right) S_1 < \frac{1}{2}$, $1 \le 2R_1 - S_1 < \frac{3}{2}$ and
$-\frac{|m|+1}{4} \le \left(\frac{|m|+1}{2}\right) S_1 - R_1 < 0$.
The result follows by taking $r = r_1 + 1$, $s = s_1$, $R = R_1 - 1$, $S = S_1$.

□

We now state our third representation.

Theorem 4.2. *Let $\gamma = a + b\sigma_m \in \mathbb{Z}[\sigma_m] \setminus \{0\}$. Let W_1 be the collection of lattice points inside the hexagon $ABCDEF$ whose vertices are, respectively,*

$$A = \frac{\gamma}{|m|}\left(\frac{3|m|-1}{4} + \frac{|m|-1}{2}\sigma_m\right),\ B = \frac{\gamma}{|m|}\left(\frac{|m|+1}{4} + \frac{|m|+1}{2}\sigma_m\right),$$
$$C = \frac{\gamma}{|m|}\left(-\frac{|m|+1}{4} + \frac{|m|-1}{2}\sigma_m\right),\ D = \frac{\gamma}{|m|}\left(-\frac{3|m|-1}{4} - \frac{|m|-1}{2}\sigma_m\right),$$
$$E = \frac{\gamma}{|m|}\left(-\frac{|m|+1}{4} - \frac{|m|+1}{2}\sigma_m\right),\ F = \frac{\gamma}{|m|}\left(\frac{|m|+1}{4} - \frac{|m|-1}{2}\sigma_m\right),$$

and let W_2 be the collection of lattice points on the line segments CD, DE and EF excluding the vertices C, F, but possibly including the endpoints D (if $D \in \mathbb{Z}[\sigma_m]$) and E (if $E \in \mathbb{Z}[\sigma_m]$). Then $W = W_1 \cup W_2$ is a $CRS(\gamma)$.

Proof. We begin by showing that any $\alpha_1 = a_1 + b_1\sigma_m \in \mathbb{Z}[\sigma_m]$ is congruent mod γ to an element in W. From Lemma 4.1, we see that $\alpha_1 \equiv (R + S\sigma_m)\gamma \pmod{\gamma}$. We show next that the point $\mathcal{P} := (R + S\sigma_m)\gamma$ belongs to the set $W = W_1 \cup W_2$. Since the line segments

AB, BC, CD, DE, EF and FA are given, respectively, by

$$\frac{\gamma}{|m|}\left\{\frac{|m|+1}{4}+\frac{|m|-1}{2}\,t+\left(\frac{|m|+1}{2}-t\right)\sigma_m\right\},$$
$$\frac{\gamma}{|m|}\left\{-\frac{|m|+1}{4}+\frac{|m|+1}{2}\,t+\left(\frac{|m|-1}{2}+t\right)\sigma_m\right\},$$
$$\frac{\gamma}{|m|}\left\{-\frac{3\,|m|-1}{4}+\frac{|m|-1}{2}\,t+\left(-\frac{|m|-1}{2}+(|m|-1)t\right)\sigma_m\right\},$$
$$\frac{\gamma}{|m|}\left\{-\frac{|m|+1}{4}+\frac{-|m|+1}{2}\,t+\left(-\frac{|m|+1}{2}+t\right)\sigma_m\right\},$$
$$\frac{\gamma}{|m|}\left\{\frac{|m|+1}{4}-\frac{|m|+1}{2}\,t+\left(-\frac{|m|-1}{2}-t\right)\sigma_m\right\},$$
$$\frac{\gamma}{|m|}\left\{\frac{3\,|m|-1}{4}+\frac{-|m|+1}{2}\,t+\left(\frac{|m|-1}{2}+(-|m|+1)\,t\right)\sigma_m\right\},$$

where $t \in \mathbb{R} \cap [0,1]$, the location of the point $\mathcal{P}$ is easily checked as follows:

- if $-\frac{|m|+1}{4} < R + \frac{|m|-1}{2}S < \frac{|m|+1}{4}$, $-1 < 2R - S < 1$, $-\frac{|m|+1}{4} < \frac{|m|+1}{2}S - R < \frac{|m|+1}{4}$, then $\mathcal{P}$ lies inside the hexagon $ABCDEF$, i.e., $\mathcal{P} \in W_1$;
- if $2R - S = -1$, then $\mathcal{P}$ lies on $\overline{CD}$ (excluding the point C), i.e., $\mathcal{P} \in W_2$;
- if $R + \frac{|m|-1}{2}S = -\frac{|m|+1}{4}$, then $\mathcal{P}$ lies on $\overline{DE}$, i.e., $\mathcal{P} \in W_2$;
- if $\frac{|m|+1}{2}S - R = -\frac{|m|+1}{4}$, then $\mathcal{P}$ lies on $\overline{EF}$ (excluding the point F), i.e., $\mathcal{P} \in W_2$.

There remains to check that any two distinct elements of W are incongruent modulo γ. To this end, let $\alpha_1 \in W$, and assume without loss of generality that it is written in standard form as

$$\frac{\alpha_1}{\gamma} = (r + s\sigma_m) + (R + S\sigma_m) = (r + R) + (s + S)\sigma_m$$

with $r, s \in \mathbb{Z}$; $R, S \in \mathbb{Q}$ satisfying (4.2)–(4.4). Since $\alpha_1 \in W$, i.e., α lies inside the hexagon or on the line segments CD, DE, EF (excluding the vertices C, F, but possibly including the points D, E), its coordinates must satisfy

$$-1 \le 2(R+r) - (S+s) < 1 \tag{4.5}$$
$$-\frac{|m|+1}{4} \le (R+r) + \left(\frac{|m|-1}{2}\right)(S+s) < \frac{|m|+1}{4} \tag{4.6}$$
$$-\frac{|m|+1}{4} \le \left(\frac{|m|+1}{2}\right)(S+s) - (R+r) < \frac{|m|+1}{4}. \tag{4.7}$$

Solving (4.2) and (4.5) and using the fact that $r, s \in \mathbb{Z}$, we get

$$2r - s = 0. \tag{4.8}$$

หลักฐานการส่งงานวิจัย

จาก : Tatiana Sworowska - Managing Editor EJM <em@editorialmanager.com>
ชื่อเรื่อง : EJMA-D-17-00127 - Submission Notification to co-author
วัน : 05-07-2017 09:51
ถึง : Suton Tadee <suton.t@tru.ac.th>;

Re: "Explicit complete residue systems in a general quadratic field"
Full author list: Vichian Laohakosol, Ph.D.; Suton Tadee, M.S.; Santad Damkaew, M.S.

Dear Mr. Tadee,

We have received the submission entitled: "Explicit complete residue systems in a general quadratic field" for possible publication in European Journal of Mathematics, and you are listed as one of the co-authors.

The manuscript has been submitted to the journal by Dr. Dr. Vichian Laohakosol who will be able to track the status of the paper through his/her login.

If you have any objections, please contact the editorial office as soon as possible. If we do not hear back from you, we will assume you agree with your co-authorship.

Thank you very much.

With kind regards,

Springer Journals Editorial Office
European Journal of Mathematics

Solving (4.3) and (4.6), we get

$$-\frac{|m|+1}{2} < r + \left(\frac{|m|-1}{2}\right) s < \frac{|m|+1}{2}. \tag{4.9}$$

Solving (4.8) and (4.9), we get

$$-|m| < -\frac{|m|+1}{2} < |m|\, r < \frac{|m|+1}{2} < |m|\,.$$

Since $r \in \mathbb{Z}$, we must have $r = s = 0$, i.e., $\alpha_1 = (R + S\sigma_m)\gamma$. Thus, any element α_2 of W is of the form

$$\alpha_2 = (U + V\sigma_m)\gamma, \quad \begin{array}{l}\text{where } U, V \text{are rational numbers satisfying (4.2)–(4.4)} \\ \text{with } U \text{ in place of } R \text{ and } V \text{ in place of } S.\end{array} \tag{4.10}$$

If $\alpha_1 \equiv \alpha_2 \pmod{\gamma}$, then $\alpha_1 = \alpha_2 + \gamma\delta$ for some $\delta \in \mathbb{Z}[\sigma_m]$. If $\delta \neq 0$, then $\gamma\delta \in \mathbb{Z}[\sigma_m] \setminus \{0\}$, which is a contradiction because α_2 is of the form (4.10) but α_1 is not. Thus, $\delta = 0$ yielding $\alpha_1 = \alpha_2$. □

Our final discussion deals with the concept of minimal representation, which is defined ([1]) as follows: a representation S of a complete residue system modulo γ is said to be an *absolute minimal representation* if and only if for any representation R of a complete residue system modulo γ, we have

$$\sum_{\alpha \in S} |N(\alpha)| \leq \sum_{\beta \in R} |N(\beta)|\,.$$

Bergum in [1] discovered an absolute minimal representation modulo γ for $\mathbb{Z}[\sigma_{-3}]$. Using our third representation, this result of Bergum is now generalized but only for the case of negative integer m.

Theorem 4.3. *Let W be as defined as in Theorem 4.2. Assume that $m < 0$. If $\alpha \in W$ and if $\beta \in \mathbb{Z}[\sigma_m]$ is such that $\beta \equiv \alpha \pmod{\gamma}$, then $|N(\beta)| \geq |N(\alpha)|$.*

Proof. From the latter half of the proof of Theorem 4.2, we can write α in its standard form as $\alpha = (R + S\sigma_m)\gamma$, with the three sets of governing inequalities (4.2)–(4.4).

Consider first the case $m \equiv 1 \pmod 4$. Since $\beta \equiv \alpha \pmod{\gamma}$, we have $\beta - \alpha = \gamma(c + d\sigma_m)$ for some $c + d\sigma_m \in \mathbb{Z}[\sigma_m]$. Therefore,

$$N\left(\frac{\beta}{\gamma}\right) = E + N\left(\frac{\alpha}{\gamma}\right),$$

where $E = 2Rc + c^2 - Rd - cS - cd + \left(\frac{1-m}{2}\right) Sd + \left(\frac{1-m}{4}\right) d^2$. To prove the theorem, it suffices to check six possibilities.

1. If $c = 0$, from (4.4), we have $E = \left(\frac{1-m}{4}\right)\left\{d^2 + d\left(\frac{-4R+(2-2m)S}{1-m}\right)\right\} \geq 0$.

2. If $c = d$, from (4.3), we have $E = \left(\frac{1-m}{4}\right)\left\{d^2 + d\left(\frac{4R+(-2-2m)S}{1-m}\right)\right\} \geq 0$.

3. If $c < d$ and $c < 0$, from (4.2), we have $2R - S - d < -d + 1 \leq -c$. Thus, $c^2 + (2R - S - d)c > 0$ and (4.4) yields

$$E = c^2 + (2R - S - d)c + \left(\frac{1-m}{4}\right)\left\{d^2 + d\left(\frac{-4R + (2-2m)S}{1-m}\right)\right\} \geq 0.$$

4. If $c < d$ and $c > 0$, from (4.4), we have $c \leq d - 1 \leq \frac{-4R+(2-2m)S}{1-m} + d$, which after simplification gives $d\left\{-R + \left(\frac{1-m}{2}\right)S + \left(\frac{1-m}{4}\right)d\right\} - \left(\frac{1-m}{4}\right)cd \geq 0$. Using $\left(\frac{-3-m}{4}\right)cd \geq 0$ and (4.2), we get

$$E = d\left\{-R + \left(\frac{1-m}{2}\right)S + \left(\frac{1-m}{4}\right)d\right\} - \left(\frac{1-m}{4}\right)cd + \left(\frac{-3-m}{4}\right)cd + (c^2 + c(2R - S)) \geq 0.$$

5. If $c > d$ and $c < 0$, from (4.4), we get $\frac{-4R+(2-2m)S}{1-m} + d < d + 1 \leq c$, which after simplification gives

$$d\left\{-R + \left(\frac{1-m}{2}\right)S + \left(\frac{1-m}{4}\right)d\right\} - \left(\frac{1-m}{4}\right)cd > 0.$$

Using $d < c < 0$ and (4.2), we have

$$E = d\left\{-R + \left(\frac{1-m}{2}\right)S + \left(\frac{1-m}{4}\right)d\right\} - \left(\frac{1-m}{4}\right)cd + \left(\frac{-3-m}{4}\right)cd + (c^2 + c(2R - S)) \geq 0.$$

6. If $c > d$ and $c > 0$, from (4.2), we have $d \leq c-1 \leq 2R-S+c$. Thus, $c(2R-S+c)-cd \geq 0$ and (4.4) yields

$$E = c(2R - S + c) - cd + \left(\frac{1-m}{4}\right)\left\{d^2 + d\left(\frac{-4R + (2-2m)S}{1-m}\right)\right\} \geq 0.$$

Next, consider the case $m \not\equiv 1 \pmod 4$. Since $\beta \equiv \alpha \pmod \gamma$, we have $\beta - \alpha = \gamma(c + d\sqrt{m})$ for some $c + d\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$. From $\frac{\beta}{\gamma} = (R + c) + (S + d)\sqrt{m}$, we get

$$N\left(\frac{\beta}{\gamma}\right) = (R + c)^2 - m\,(S + d)^2 = N\left(\frac{\alpha}{\gamma}\right) + E, \tag{4.11}$$

where $E = 2Rc + c^2 - 2mSd - md^2$. Since $R, S \in [-1/2, 1/2)$, and c, d, m are rational integers with m being negative, we have $E = (c^2 + 2Rc) - m(d^2 + 2Sd) \geq 0$. Thus, (4.11) implies $|N(\beta)| \geq |N(\alpha)|$.

□

5 Acknowledgments

The first author is supported by the Faculty of Science and Technology, Thepsatri Rajabhat University. The second author is supported by the Center for Advanced Studies in Industrial Technology and the Faculty of Science, Kasetsart University.

References

[1] G. E. Bergum. Complete residue systems in the quadratic domain $\mathbb{Z}(e^{2\pi i/3})$, Internat. J. Math. Math. Sci. 1 (1978), 75–86.

[2] N. R. Hardman and J. H. Jordan, A minimum problem connected with complete residue systems in the Gaussian integers, Amer. Math. Monthly 74 (1967), 559–561.

[3] H. Pollard and H. G. Diamond, The Theory of Algebraic Numbers, The Mathematical Association of America, 1975

[4] J. H. Jordan and C. J. Potratz, Complete residue systems in the Gaussian integers, Math. Magazine 38 (1965), 1–12.

[5] C. J. Potratz, Character sums in $\mathbb{Z}(\sqrt{-2})/(p)$, Ph.D. dissertation, Washington State University, 1966.

[6] D. Redmond, Number Theory, An Introduction, Marcel Dekker, New York, 1996.