Divulgaciones Matemáticas Vol. 18 No. 2 (2017), pp. 1–17

Explicit complete residue systems in a general quadratic field

Sistemas de residuos completos explícitos en un cuerpo cuadrático en general

Suton Tadee (suton.t@tru.ac.th)
Department of Mathematics, Faculty of Science and Technology,
Thepsatri Rajabhat University, Lopburi 15000, Thailand

Vichian Laohakosol (fscivil@ku.ac.th)
Department of Mathematics, Faculty of Science,
Kasetsart University, Bangkok 10900, Thailand

Santad Damkaew (s.damkaew@hotmail.co.th)
Department of Mathematics and Computer Science, Chulalongkorn University,
Bangkok 10330, Thailand

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 phrases: quadratic field, complete residue system, lattice point.

Resumen

Bergum determinó explícitamente tres representaciones para un sistema de residuo completo en el cuerpo cuadrático $\mathbb{Q}\left(\sqrt{-3}\right)$ extendiendo dos resultados anteriores en $\mathbb{Q}\left(\sqrt{-1}\right)$ y $\mathbb{Q}\left(\sqrt{-2}\right)$. Entre estas tres representaciones, la primera es más simple de obtener, mientras que la tercera es mínima en el sentido de que la suma de sus valores absolutos es mínimo. Aquí, ampliamos estos resultados obteniendo representaciones explícitas para un sistema completo de residuos en cualquier cuerpo cuadrático general. La primera representación usa puntos reticulares en un rectángulo en el primer cuadrante de un plano apropiado, mientras que la segunda representación utiliza puntos reticulares en un paralelogramo y la tercera representa puntos reticulares en un hexágono y posee una propiedad de minimalidad para cuerpos cuadráticos imaginarios.

Palabras y frases clave: cuerpos cuadráticos, sistema completo de residuos, punto reticular.

Received 17/08/2017. Revised 30/08/2017. Accepted 05/12/2017.
MSC (2000): Primary 11A07; Secondary 11R04.

1 Introduction

The problem of explicitly determining complete residue systems in a general number field is nontrivial, 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, $m \notin \{0, 1\}$;

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

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

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 $c = -dl\left(a_1^2 - mb_1^2\right)$, 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*

$$T_1 ;= \left\{ x + y\sqrt{m} : \ x, y \in \mathbb{Z}, \ 0 \le x \le d\,|N(\mu)| - 1, \ 0 \le y \le \frac{d-1}{2} \right\}$$
$$T_2 := \left\{ \left(x + \frac{1}{2}\right) + \left(y + \frac{1}{2}\right)\sqrt{m} : \ x, y \in \mathbb{Z}, \ 0 \le x \le d\,|N(\mu)| - 1, \ 0 \le y \le \frac{d-3}{2} \right\},$$

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 $x_i, y_i \in \mathbb{Z}$, $0 \leq x_i \leq d\,|N(\mu)| - 1$, $0 \leq y_i \leq \frac{d-2}{2}$ $(i = 1, 2)$. 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

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

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

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

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 $0 \leq n_2 < d\,|N(\mu)|\,$, $0 \leq r_1 = 2n_1 < d$, and d is even, we have $0 \leq n_2 \leq d\,|N(\mu)| - 1$, $0 \leq n_1 \leq (d - 2)/2$. 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

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

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 $0 \leq n_2 < d\,|N(\mu)|$ and $0 \leq n_1 = \frac{r_1-1}{2} \leq \frac{d-2}{2}$, 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

$$C_1 := \begin{cases} \left(a_1 a - a_1 b + \frac{1-m}{4} b_1 b\right)/N(\gamma) & \text{if } m \equiv 1 \pmod 4\\ \left(a_1 a - b_1 bm\right)/N(\gamma) & \text{if } m \not\equiv 1 \pmod 4\end{cases}$$

and $D_1 := (b_1 a - a_1 b)\,/N(\gamma)$. 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,*

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

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

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

iii.6) $\frac{|m|-3}{4} \le R_1 + \left(\frac{|m|-1}{2}\right) S_1 < \frac{|m|-1}{4},\ -3/2 < 2R_1 - S_1 < -1$ and
$\frac{|m|+1}{4} \le \left(\frac{|m|+1}{2}\right) S_1 - R_1 < \frac{|m|+3}{4}.$
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

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

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

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,*

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

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

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

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

$$-1 \leq 2(R + r) - (S + s) < 1 \tag{4.5}$$

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

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

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

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

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

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

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 $\beta \equiv \alpha$ (mod γ), 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
$$\begin{aligned} E = d&\left\{-R + \left(\frac{1-m}{2}\right)S + \left(\frac{1-m}{4}\right)d\right\} - \left(\frac{1-m}{4}\right)cd + \left(\frac{-3-m}{4}\right)cd \\ &+ (c^2 + c(2R - S)) \geq 0. \end{aligned}$$

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

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.