ON SYMMETRIC RADIX REPRESENTATION
OF GAUSSIAN INTEGERS

GABRIELE STEIDL

Wilhelm-Pieck-Universität Rostock, Sektion Mathematik, Universitätsplatz 1, DDR-2500 Rostock, German Democratic Republic.

Abstract.

Symmetric radix representation and symmetric mixed-radix representation of Gaussian integers play a significant role in the residue arithmetic of $\mathbb{Z}[i]$. In the following, known results concerning corresponding representations of integers are generalized. It is shown that for any modulus $m \in \mathbb{Z}[i]$ with $m^2 > 1$, except for $m = 1 \pm i, 2$, there exists a unique symmetric $m$-radix representation of Gaussian integers.

AMS Subject Classification: 11A63.

CR Categories: F.2.1., G.1.0.

Keywords: Gaussian integers, symmetric residue, symmetric radix representation, symmetric mixed-radix representation, residue arithmetic, complex number system.

1. Introduction.

Let us denote by $\mathbb{Z}$ the ring of integers, by $\mathbb{N}$ the set of positive integers and by $\mathbb{C}$ the field of complex numbers. Let $m \in \mathbb{Z} \,(m > 1)$. For any $a \in \mathbb{Z}$, the symmetric residue $|a|_m$ of $a \in \mathbb{Z}$ modulo $m$ [9, p. 113] is defined by

$$a \equiv |a|_m \,(\text{mod} \, m), \quad -m/2 < |a|_m \leq m/2.$$

The following theorems are well known.

**Theorem 1.1:** Let $m \in \mathbb{Z} \,(m > 1)$, and let $n \in \mathbb{N}$ be given. Then any $a \in \mathbb{Z}$ with $a = |a|_m$ has a unique representation of the form

$$a = a_0 + a_1 m + \ldots + a_{n-1} m^{n-1} + qm^n$$

with symmetric $m$-radix digits $a_j = |a_j|_m, \quad (j = 0, \ldots, n - 1)$ and with

$$q = \begin{cases} -1 & \text{if } 2 \mid m \text{ and } a < -(m - 2)(m^n - 1)/2(m - 1), \\ 0 & \text{otherwise.} \end{cases}$$

Received January 1989.
For odd \( m \in \mathbb{Z} \) (\( m > 1 \)), the proof of Theorem 1.1 is given in [3]. In the case when \( m > 1 \) is an even integer, the assertion can be shown similarly. One has only to observe that for even \( m \in \mathbb{Z} \) the range of integers representable in the form (1.1) with \( q = 0 \) is \([- (m - 2)(m^n - 1)/2(m - 1), m(m^n - 1)/2(m - 1)]\), since

\[
- \frac{(m - 2)(m^n - 1)}{2(m - 1)} = - \frac{m - 2}{2} - \frac{m - 2}{2} \frac{m - \ldots - m - 2}{m - 1} m^n - 1
\]

\[
\leq a_0 + a_1 m + \ldots + a_{n-1} m^n - 1
\]

\[
\leq \frac{m}{2} + \frac{m}{2} m + \ldots + \frac{m}{2} m^n - 1 = \frac{m(m^n - 1)}{2(m - 1)}.
\]

If for \( m \in \mathbb{Z} \), any \( a \in \mathbb{Z} \) can be uniquely represented in the form (1.1) with some \( n \in \mathbb{N} \) and \( q = |q|_m \), then we say that there exists a symmetric \( m \)-radix representation in \( \mathbb{Z} \). Clearly, by Theorem 1.1, for any \( m \in \mathbb{Z} \) with \( m > 2 \), there exists a symmetric \( m \)-radix representation in \( \mathbb{Z} \).

**Theorem 1.2** [3]: Let \( m_j \in \mathbb{Z}, m_j > 1 \) (\( j = 1, \ldots, s \)) be pairwise relatively prime odd integers. Set \( m := m_1 \ldots m_s \). Then any \( a \in \mathbb{Z} \) with \( a = |a|_m \) has a unique symmetric mixed-radix representation of the form

\[
a = a^{(0)} + a^{(1)} m_1 + \ldots + a^{(s)} m_1 \ldots m_s
\]

with symmetric mixed-radix digits \( a^{(j)} = |a^{(j)}| m_j \) (\( j = 1, \ldots, s \)).

The above theorems not only play a significant role in computational number theory, they are also important in connection with fast algorithms for numerical problems, for instance, for the exact solution of linear equations [2,3]; for fast number-theoretic transforms and cyclic convolutions [6, 8] or for the implementation of a fast arithmetic in \( \mathbb{Z} \) based on the Chinese Remainder Theorem. During the last years, such numerical tasks have received attention for the ring \( \mathbb{Z}[i] \) (\( i^2 = -1 \)) of Gaussian integers [6, 7]. In this paper, we extend Theorems 1.1 and 1.2 to complex integers by using a symmetric residue representation in \( \mathbb{Z}[i] \), which for practical purposes seems more suitable than the residue representation given in [4]. Further, we correct the results in [1, pp. 75–77].

2. Symmetric residues in \( \mathbb{Z}[i] \).

We denote by \( \bar{x} \) the conjugate complex number of \( x \in \mathbb{C} \). The norm \( N(x) \) of \( x = \text{Re}(x) + i \text{Im}(x) \in \mathbb{C} \) is defined by

\[
N(x) = xx^\bar{} = |x|^2 = \text{Re}(x)^2 + \text{Im}(x)^2.
\]

Let \( m \in \mathbb{Z}[i] \) (\( N(m) > 1 \)). Given any \( z \in \mathbb{Z}[i] \), if \( z \equiv r \, (\text{mod } m) \) and if

\[
-1/2 < \text{Re}(r/m), \quad \text{Im}(r/m) \leq 1/2,
\]
then we write \( r = |z|_m \), and say that \( |z|_m \) is the symmetric residue of \( z \in \mathbb{Z}[i] \) modulo \( m \) [1, pp. 41–42]. By (2.1), condition (2.2) is equivalent to

\[
-\frac{N(m)}{2} < \text{Re}(r\bar{m}), \quad \text{Im}(r\bar{m}) \leq \frac{N(m)}{2}.
\]

In the case that \( m \in \mathbb{Z} \) (\( m > 1 \)), it holds for any \( z \in \mathbb{Z}[i] \)

\[
|z|_m = |\text{Re}(z)|_m + i|\text{Im}(z)|_m.
\]

If \( m \), \( z \in \mathbb{Z} \) (\( m > 1 \)), then the definition of the symmetric residue in \( \mathbb{Z}[i] \) coincides with that in \( \mathbb{Z} \). The following lemma implies that \( |z|_m \) is uniquely determined, and that \( |z|_m \) can be calculated by real operations.

**Lemma 2.1:** Let \( m \in \mathbb{Z}[i] \) (\( N(m) > 1 \)), and let \( z \in \mathbb{Z}[i] \) be given. Then \( |z|_m \) can be computed by

\[
|z|_m = (|\text{Re}(z\bar{m})|_{N(m)} + i|\text{Im}(z\bar{m})|_{N(m)})m/N(m).
\]

**Proof.** Let \( r := |z|_m \). Then \( z = mq + r \) with some \( q \in \mathbb{Z}[i] \). Hence \( z\bar{m} = N(m)q + r\bar{m} \), which implies by (2.3) that

\[
|\text{Re}(z\bar{m})|_{N(m)} = |\text{Re}(r\bar{m})|_{N(m)} = \text{Re}(r\bar{m}),
\]

\[
|\text{Im}(z\bar{m})|_{N(m)} = |\text{Im}(r\bar{m})|_{N(m)} = \text{Im}(r\bar{m}).
\]

Thus \( rm = |\text{Re}(rm)|_{N(m)} + i|\text{Im}(rm)|_{N(m)} \). By (2.1), this yields the assertion.

By \( R(m) := \{ z \in \mathbb{Z}[i] : z = |z|_m \} \), we denote the set of all symmetric residues modulo \( m \). Later we use the numbers of \( R(m) \) as symmetric \( m \)-radix digits. Regarding that \( z \in R(m) \) if and only if \( z \) fulfils (2.3), it is easy to verify that \( \text{card}(R(m)) = N(m) \).

---

**Fig. 1.** \( G \), \( G(m) \) and \( R(m) \) for \( m = 3 + i \).

(The dashed lines do not belong to \( G \) and \( G(m) \), respectively.)
Let us consider $R(m)$ from the geometrical point of view. Set
\[ G := \{ x \in \mathbb{C} : -1/2 < \text{Re}(x), \text{Im}(x) \leq 1/2 \}, \]
\[ G(m) := \{ xm \in \mathbb{C} : x \in G \}. \]

Since the Gaussian integers are the lattice points of $\mathbb{C}$, it follows by (2.2) that $R(m)$ consists of all lattice points of $G(m)$. See Figure 1.

In Section 3, we use the obvious

**Lemma 2.2:** Let $m \in \mathbb{Z}[i]$ ($N(m) > 1$). Then it holds for any $x \in \mathbb{C}$:

i) If $x \in G(m)$, then $|x| \leq (\sqrt{2}/2)|m|$. If $|x| < |m|/2$, then $x \in G(m)$.

ii) There exists $n \in \mathbb{N}$, such that $x \in G(m^n)$.

The following lemma shows the symmetry property of $R(m)$.

**Lemma 2.3:** Let $m \in \mathbb{Z}[i]$ with odd norm $N(m) > 1$. If $z \in R(m)$, then $\alpha z \in R(m)$ for $\alpha \in \{ \pm 1, \pm i \}$.

The proof of Lemma 2.3 follows by (2.3), regarding that for $m \in \mathbb{Z}[i]$ with odd norm $N(m) > 1$, it holds $z \in R(m)$ if and only if $|\text{Re}(zn)|, |\text{Im}(zn)| < N(m)/2$.

As in Section 1, we say for $m \in \mathbb{Z}[i]$, that there exists a symmetric $m$-radix representation in $\mathbb{Z}[i]$, if any $z \in \mathbb{Z}[i]$ can be uniquely represented as
\[ z = z_0 + z_1 m + \ldots + z_n m^n \]
with some $n \in \mathbb{N}$ and symmetric $m$-radix digits $z_j \in R(m) (j = 0, \ldots, n)$.

### 3. Main results.

In this section, we show that for any modulus $m \in \mathbb{Z}[i]$ ($N(m) > 1$), except for $m = 1 \pm i, 2$, there exists a symmetric $m$-radix representation in $\mathbb{Z}[i]$, which has some special features compared with that in $\mathbb{Z}$.

**Theorem 3.1:** Let $m \in \mathbb{Z}[i]$ ($N(m) > 1$), and let $n \in \mathbb{N}$ be given. Then every $z \in \mathbb{Z}[i]$ with $z = |z|M_m$ has a unique representation of the form
\[ z = |z_0| + z_1 m + \ldots + z_{n-1} m^{n-1} |m^n \]
with symmetric $m$-radix digits $z_j \in R(m) (j = 0, \ldots, n - 1)$.

**Proof.** Let $z \in \mathbb{Z}[i]$ with $z = |z|M_m$. Then there exists a uniquely determined $q_1 \in \mathbb{Z}[i]$, such that $z = q_1 m + |z|_m$. We set $z_0 := |z|_m$ and consider $q_1 = (z - z_0)/m$. Again, there exists a uniquely determined $q_2 \in \mathbb{Z}[i]$, such that $q_1 = q_2 m + |q_1|_m$.
Repeating these considerations successively for \( z_j := |q_j|_m \),

\[
q_{j+1} := \frac{q_j - z_j}{m} = \frac{z}{m^{j+1}} - \frac{z_0}{m^{j+1}} \frac{z_1}{m^j} - \cdots - \frac{z_j}{m} \quad (j = 1, \ldots, n - 1),
\]

we obtain

\[
q_n = \frac{z}{m^n} - \frac{z_0}{m^n} - \frac{z_1}{m^{n-1}} - \cdots - \frac{z_{n-1}}{m} \in \mathbb{Z}[i].
\]

Thus

\[
z = z_0 + z_1 m + \ldots + z_{n-1} m^{n-1} + q_n m^n,
\]

where \( z_j \in R(m) \) \((j = 0, \ldots, n - 1)\) and \( q_n \in \mathbb{Z}[i] \) are uniquely determined. By \( z = |z|_m \),
this yields the assertion. \( \blacksquare \)

By the following example, we see that the reduction modulo \( m^n \) on the right side of (3.1) cannot be neglected.

**Example 3.1:** Let \( m = 1 + 2i \). We have \( R(1 + 2i) = \{0, \pm 1, \pm i\} \). Then

\[
z = 3i = 3i1(1 + 20^2 = i(1 + 20 + 11(1+20^2 = (1 + 2i)^2 - i(1 + 2i) + 1.
\]

But 3i has no representation of the form \( z_0 + z_1(1 + 2i) \) with \( z_j \in R(1 + 2i) \) \((j = 0, 1)\).

In general, we obtain as extension of Theorem 1.1 to \( \mathbb{Z}[i] \):

**Theorem 3.2:** Let \( m \in \mathbb{Z}[i] \) \((N(m) \geq 5)\), and let \( n \in \mathbb{N} \) be given. Then any \( z \in \mathbb{Z}[i] \) with \( z = |z|_m \) has a unique representation of the form

\[
z = z_0 + z_1 m + \ldots + z_{n-1} m^{n-1} + q m^n
\]

with symmetric \( m \)-radix digits \( z_j \in R(m) \) \((j = 0, \ldots, n - 1)\) and with \( q \in S := \{0, \pm 1, \pm i, \pm 1 \pm i\} \).

**Proof.** By the proof of Theorem 3.1, \( z \in \mathbb{Z}[i] \) can be represented uniquely in the form (3.2) with \( z_j \in R(m) \) \((j = 0, \ldots, n - 1)\) and with some \( q \in S \). By (3.2), we obtain

\[
q = z/m^n - \sum_{j=0}^{n-1} z_j/m^{n-j}.
\]

Thus

\[
|q| \leq |z/m^n| + \sum_{j=0}^{n-1} |z_j/m| |1/m^{n-1-j}|.
\]

Using Lemma 2.2i), we verify by assumption of \( z \) and \( z_j \) that

\[
|q| \leq (\sqrt{2}/2) \left( 1 + \sum_{j=0}^{n-1} 1/|m|^j \right) < (\sqrt{2}/2)(1 + |m|/(|m| - 1)) < 2
\]
for $m \in \mathbb{Z}[i]$ with $N(m) \geq 5$. Hence $N(q) < 4$, which is fulfilled exactly for the Gaussian integers $q \in S$. $
abla$

Note that the summand $qm^n$ does not vanish in general in (3.2). This important fact was not observed in [1], which led to false results. Indeed, for any $q \in S$, one can find $m \in \mathbb{Z}[i]$ with odd norm $N(m) \geq 5$, $n \in N$ and $z \in \mathbb{Z}[i]$ with $z = |z|_{m^n}$ satisfying (3.2).

EXAMPLE 3.2: Let $m = 1 + 2i$. By Example 3.1 and Lemma 2.3, we obtain desired representations (3.2) with $q \in \{ \pm 1, \pm i \}$.

Further, we have

$$z = -124 + 153i = (-124 + 153i)(1 + i)m^7 - m^6 + m^5 + im^4 - m^3 - im^2 + m + i,$$

i.e. $q = 1 + i$. By Lemma 2.3, we get representations (3.2) with $q \in \{-1 \pm i, 1 - i\}$ for $z = (-124 + 153i)\alpha$ with $\alpha \in \{-1, \pm i\}$.

In the case $m \in \mathbb{Z}[i]$ with even norm $N(m) \geq 8$, we get by the following lemmata $q \in S \backslash \{-1 + i, 1 \pm i\}$ in (3.2).

**LEMMA 3.3:** Let $x = a + bi$, $y = c + di \in \mathbb{C}$ ($y \neq 0$). Then it holds

$$\left| \Re \left( \frac{x}{y} \right) \right|, \left| \Im \left( \frac{x}{y} \right) \right| \leq \sqrt{2} |y|^{-1} \max \{|a|, |b|\}.$$

**PROOF.** First, we have by

$$(|c| + |d|)/2 \leq (c^2 + d^2)/2^{1/2} = |y|/\sqrt{2}$$

(3.4) $$\frac{|c| + |d|}{N(y)} \leq \frac{\sqrt{2}}{|y|}.$$

Further, we obtain

$$\left| \Re \left( \frac{x}{y} \right) \right| = \frac{|ac + bd|}{N(y)} \leq \frac{|ac| + |bd|}{N(y)} \leq \frac{|c| + |d|}{N(y)} \max \{|a|, |b|\},$$

$$\left| \Im \left( \frac{x}{y} \right) \right| = \frac{|ad - bc|}{N(y)} \leq \frac{|ad| + |bc|}{N(y)} \leq \frac{|c| + |d|}{N(y)} \max \{|a|, |b|\}. $$

By (3.4), this yields the assertion. $

**LEMMA 3.4:** Let $m \in \mathbb{Z}[i]$ with even norm $N(m) \geq 8$, and let $n \in N$ be given. Then any $z \in \mathbb{Z}[i]$ with $z = |z|_{m^n}$ has a unique representation of the form (3.2) with symmetric $m$-radix digits $z_j \in R(m)$ and with $q \in \{0, \pm 1, \pm i, -1 - i\}$. 

PROOF. By Theorem 3.2, it remains to show that $q \notin \{-1 + i, 1 \pm i\}$. By (3.2), we get for

$$r := \frac{z_0}{m^{n-1}} + \frac{z_1}{m^{n-2}} + \cdots + \frac{z_{n-2}}{m}$$

that

$$r = \left(\frac{z}{m^{n-1}} - qm\right) - z_{n-1}.$$

Assume that there exists $z \in \mathbb{Z}[i]$ with $z = |z|_m$, such that $q \in \{-1 + i, 1 \pm i\}$ in (3.2). Since $N(m)$ is even, we have $(\pm 1 \pm i)m/2 \in \mathbb{Z}[i]$. Therefore, and since $qm/2 \notin R(m)$, we obtain for any $x \in G(m) - qm$ and for any $y \in R(m)$ that

$$|\text{Re}(x - y)| \geq 1 \quad \text{or} \quad |\text{Im}(x - y)| \geq 1.$$

See Figure 2. Hence we have by $z/m^{n-1} - qm \in G(m) - qm$ and by $z_{n-1} \in R(m)$ that

(3.5) \quad $|\text{Re}(r)| \geq 1 \quad \text{or} \quad |\text{Im}(r)| \geq 1$.

On the other hand, it holds

$$|\text{Re}(r)| \leq \sum_{j=0}^{n-2} |\text{Re}(z_j/m^{n-1-j})|, \quad |\text{Im}(r)| \leq \sum_{j=0}^{n-2} |\text{Im}(z_j/m^{n-1-j})|,$$

Fig. 2. $G(m)$ and $G(m) - (\pm 1 \pm i)m$ for $m = 3 + i$.  

---

**Fig. 2.** $G(m)$ and $G(m) - (\pm 1 \pm i)m$ for $m = 3 + i$. 

---
which by (2.2) and Lemma 3.3 implies
\[ |\text{Re}(r)|, |\text{Im}(r)| \leq \frac{1}{2} \sum_{j=0}^{n-2} (\sqrt{2}/|m|)^j < |m|/2(|m| - \sqrt{2}) \leq 1 \]
if \( N(m) \geq 8 \). But this contradicts (3.5). \( \blacksquare \)

For practical purposes, especially in connection with fast complex number-theoretic transforms, it is often suitable to use rational integers \( m \) as moduli for symmetric radix representations.

**Lemma 3.5:** Under the assumptions of Theorem 3.2, it holds:

i) If \( m \in \mathbb{Z} \) (\( m > 1 \)) is odd, then \( q = 0 \) in (3.2).

ii) If \( m \in \mathbb{Z} \) (\( m > 1 \)) is even, then
\[
q = \begin{cases} 
0 & \text{if } \text{Re}(z), \text{Im}(z) \geq M, \\
-1 & \text{if } \text{Re}(z) < M, \text{Im}(z) \geq M, \\
-i & \text{if } \text{Re}(z) \geq M, \text{Im}(z) < M, \\
-1 - i & \text{otherwise},
\end{cases}
\]
with \( M := -(m - 2)(m^n - 1)/2(m - 1) \).

**Proof.** Since \( m \in \mathbb{Z} \), we obtain the assertion based on (2.4) by applying Theorem 1.1 to \( \text{Re}(z) \) and \( \text{Im}(z) \), separately. \( \blacksquare \)

For the next theorem, we need some further preparations. We use the notations of Theorem 3.2. Then for \( m \in \mathbb{Z}[i] \) with \( N(m) > 8 \), \( q = |q|_m \), and for \( m \in \mathbb{Z}[i] \) with \( 5 \leq N(m) \leq 8 \), \( q \in S \) can be represented as \( q = r_0 + r_1 m \) with \( r_j \in \mathbb{R}(m) \) (\( j = 0,1 \)). Further, by (3.3), any \( z \in \mathbb{Z}[i] \) with \( z = |z|_m \) can be written in the form (3.3) with
\[
q \in S_1 = S \cup \{ \pm 2, \pm 2i \} \quad \text{if} \quad N(m) = 4,
q \in S_2 = S \cup \{ \pm 2, \pm 2i, \pm 3, \pm 3i \} \quad \text{if} \quad N(m) = 2.
\]

In the case \( q \in S_1 \), one can check that except for \( m = 2 \), the elements of \( S_1 \) can be represented as \( q = r_0 + r_1 m + r_2 m^2 \) with \( r_j \in \mathbb{R}(m) \) (\( j = 0,1,2 \)). If \( m \in \mathbb{Z}[i] \) with \( N(m) = 2 \) and if \( m \neq 1 \pm i \), then any \( q \in S_2 \) can be written uniquely as \( q = r_0 + r_1 m + \ldots + r_7 m^7 \) with \( r_j \in \mathbb{R}(m) \) (\( j = 0, \ldots, 7 \)).

Finally, note that it is not possible to find a representation \( q = r_0 + r_1 m + \ldots + r_n m^n \) with some \( n \in \mathbb{N} \) and \( r_j \in \mathbb{R}(m) \) (\( j = 0, \ldots, n \)) for \((q,m) = (-1,1+i), (-i,1-i), (-1,2)\).

Regarding Theorem 3.2 and Lemma 2.2ii), we summarize our main result on the symmetric \( m \)-radix representation in \( \mathbb{Z}[i] \).

**Theorem 3.6:** Except for \( m = 1 \pm i,2 \), there exists a symmetric \( m \)-radix representation in \( \mathbb{Z}[i] \) for any modulus \( m \in \mathbb{Z}[i] \) (\( N(m) > 1 \)).
Compared with [4], we see that \((m, R(m))\) is a so-called “complex number system” for arbitrary \(m \in \mathbb{Z}[i]\) \((N(m) > 1, m \neq 1 \pm i, 2)\). Hence, for computational purposes, these systems are more suitable than the complex number systems \((m, \{0, 1, \ldots, N(m) - 1\})\) introduced in [4], where one has to choose \(m \in \{-a \pm i : a \in \mathbb{N}\}\).

With respect to Theorem 1.2, we state

**Theorem 3.7:** Let \(m_j \in \mathbb{Z}[i]\) with \(N(m_j) > 1\) \((j = 1, \ldots, s)\) be pairwise relatively prime. Set \(m := m_1 \ldots m_s\). Then any \(z \in \mathbb{Z}[i]\) with \(z = |z|_m\) has a unique representation of the form

i) \(z = \left|z^{(1)} + z^{(2)} m_1 + \ldots + z^{(a)} m_1 \ldots m_{s-1}\right|_m\),

ii) \(z = z^{(1)} + z^{(2)} m_1 + \ldots + z^{(a)} m_1 \ldots m_{s-1} + q m\) \((q \in \mathbb{Z}[i])\)

with symmetric mixed-radix digits \(z^{(j)} \in R(m_j)\) \((j = 1, \ldots, s)\) and with \(q \in S\) if \(N(m_j) > 5\) \((j = 1, \ldots, s)\).

The proof of part i) follows directly from the Chinese Remainder Theorem [5, pp. 280–282]. Theorem 3.7ii) can be shown in a similar way as Theorem 3.2.

Note that \(q = 0\) in ii), if all moduli \(m_j > 1\) \((j = 1, \ldots, s)\) are odd rational integers.

**REFERENCES**