Canad. Math. Bull. Vol. 69 (2), 2026, pp. 688–701
http://dx.doi.org/10.4153/S0008439525101331
© Institute for Defense Analyses, 2025. Published by Cambridge University Press on behalf of Canadian Mathematical Society

# A division algorithm for the Gaussian integers' minimal Euclidean function

Hester Graves

*Abstract.* The usual division algorithms on $\mathbb{Z}$ and $\mathbb{Z}[i]$ measure the size of remainders using the algebraic norm. These rings are Euclidean with respect to several functions. The pointwise minimum of all Euclidean functions $f : R\backslash\{0\} \to \mathbb{N}$ on a Euclidean domain $R$ is itself a Euclidean function, called the minimal Euclidean function and denoted by $\phi_R$. To the author's knowledge, the integers, $\mathbb{Z}$ and the Gaussians, $\mathbb{Z}[i]$ are the only rings of integers of number fields for which we have a formula to compute their minimal Euclidean functions, $\phi_{\mathbb{Z}}$ and $\phi_{\mathbb{Z}[i]}$. This article presents the first division algorithm (that the author knows of) for $\mathbb{Z}[i]$ relative to $\phi_{\mathbb{Z}[i]}$, empowering readers to perform the Euclidean algorithm on $\mathbb{Z}[i]$ using its minimal Euclidean function.

## 1 Introduction

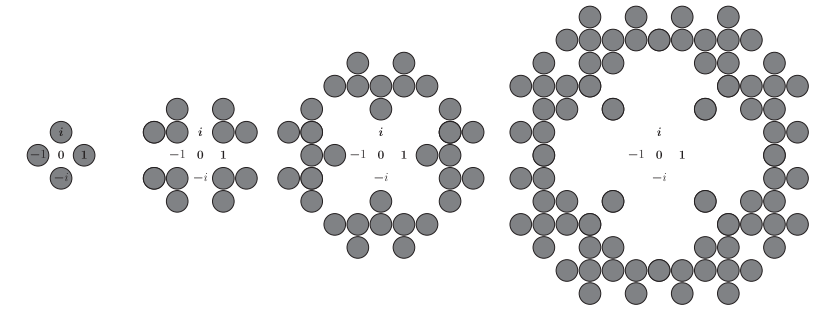
We call $\mathbb{Z}[i] = \{x + yi : x, y \in \mathbb{Z}, i^2 = -1\}$ the Gaussian integers because Gauss showed the domain has unique factorization. Due to Dirichlet's realization that Euclidean rings have unique factorization, we say the Gaussian integers form a unique factorization domain because they are Euclidean for the algebraic (or field) norm, $\mathrm{Nm}(x + yi) = x^2 + y^2$. The standard proof that $\mathbb{Z}[i]$ is Euclidean uses a division algorithm that, given $a, b \in \mathbb{Z}[i]\backslash\{0\}$, provides $q, r \in \mathbb{Z}[i]$ such that $a = qb + r$ and $\mathrm{Nm}(r) < \frac{\mathrm{Nm}(b)}{2}$ (see Equation (2.2)). Accordingly, we call $r$ the Gauss remainder for $a$ and $b$.

Inspired by Zariski, Motzkin [3] broadened the study of Euclidean domains via Euclidean functions. A domain $R$ is Euclidean if there exists a *Euclidean function* $f : R\backslash\{0\} \to W$, where $W$ is a well-ordered set with $\mathbb{N}$ as an initial segment, such that for all $a, b \in R\backslash\{0\}$, there exist some $q, r \in R$ such that $a = qb + r$, where either $f(r) < f(b)$ or $r = 0$. Using this modern terminology, the algebraic norm is a Euclidean function for $\mathbb{Z}[i]$.

Motzkin [3] further showed that if $F$ is the set of all Euclidean functions on $R\backslash\{0\}$, then $\phi_R(x) = \min_{f\in F} f(x)$ is itself a Euclidean function. For obvious reasons, we call $\phi_R$ the *minimal Euclidean function* on $R$. In particular, he showed $\phi_{\mathbb{Z}}(x) = \lfloor \log_2 |x| \rfloor$. Until 2023, this was the only formula the author knew of to compute the minimal Euclidean function for any number field.

Received by the editors March 3, 2025; revised September 17, 2025; accepted September 17, 2025.
Published online on Cambridge Core October 30, 2025.
AMS subject classification: **11A05**, **11R99**, 11A63, 11R04, 11R11, 11R18.
Keywords: Number theory, Euclidean algorithm, Euclidean function, Gaussian integers, quadratic number fields.

https://doi.org/10.4153/S0008439525101331 Published online by Cambridge University Press



(a) $\phi^{-1}_{\mathbb{Z}[i]}(0)$ (b) $\phi^{-1}_{\mathbb{Z}[i]}(1)$ (c) $\phi^{-1}_{\mathbb{Z}[i]}(2)$ (d) $\phi^{-1}_{\mathbb{Z}[i]}(3)$

*Figure 1*: Pre-images of $\phi_{\mathbb{Z}[i]}$.

Just as every integer has a binary expansion, every Gaussian integer has $(1+i)$-ary expansions. This is fitting, as $2 = -i(1+i)^2$ and the quotient $\mathbb{Z}[i]/\langle 1+i\rangle$ has size 2. We use $(1+i)$-expansions of the form $x+yi = \sum_{j=0}^{n} u_j(1+i)^j$ for some $n$, where $u_j \in \{\pm 1, \pm i, 0\}$ and $u_n \neq 0$. These expressions are not unique, as

$$2 + i = -i(1+i)^2 + i = (1+i) + 1. \tag{1.1}$$

Lenstra, Jr. [2, Section 11] showed that $\phi_{\mathbb{Z}[i]}(x+yi)$ is the minimal degree of all $(1+i)$-ary expansions of $x+yi$, e.g., $\phi_{\mathbb{Z}[i]}(2+i) = \deg_{1+i}((1+i)+1) = 1$. Therefore, if $x+yi \in \mathbb{Z}[i]\backslash\{0\}$, then $\phi_{\mathbb{Z}[i]}((1+i)^n x) = \phi_{\mathbb{Z}[i]}(x) + n$ and $\phi_{\mathbb{Z}[i]}(ux) = \phi_{\mathbb{Z}[i]}(x)$ for all $u$ in $\mathbb{Z}[i]$'s group of multiplicative units, $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. He did not, however, provide methods to calculate $\phi_{\mathbb{Z}[i]}$ for a generic $x+yi \in \mathbb{Z}[i]\backslash\{0\}$; Equation (1.1) shows computing $\phi_{\mathbb{Z}[i]}$ is not straightforward.

The author's recent research gives an explicit formula for $\phi_{\mathbb{Z}[i]}(x+yi)$, using valuations and the sequence $\{w_m\}$ [1]. Figure 1 shows which Gaussian integers map to $\{0,1,2,3\}$ under $\phi_{\mathbb{Z}[i]}$. An explanation of this work requires a great deal of notation.

## 1.1 Notations and definitions

### 1.1.1 Notation

- Every complex number has a real and imaginary part, denoted by $\mathrm{Re}(x+yi) = x$ and $\mathrm{Im}(x+yi) = y$.
- The complex conjugate of $z$ is $\overline{z} = \mathrm{Re}(z) - \mathrm{Im}(z)i$.
- The algebraic norm of $z = x+yi \in \mathbb{Q}(i)$ is $z \cdot \overline{z} = x^2 + y^2$.
- If $a$ divides $b$, we write $a|b$. Otherwise, $a \nmid b$.
- When $a^c|b$ but $a^{c+1} \nmid b$, we say $c$ is the $a$-valuation of $b$, or $v_a(b) = c$ ([1], p 25).
- We use $\gcd(x,y)$ to denote the greatest common divisor of $x$ and $y$.
- For $x \in \mathbb{R}$, $\mathrm{sgn}(x) = \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \\ -1 & \text{if } x < 0. \end{cases}$
- The $\ell_1$-norm is $\ell_1(x+yi) = |x| + |y|$ and the $\ell_\infty$-norm is $\ell_\infty(x+yi) = \max(|x|, |y|)$.

https://doi.org/10.4153/S0008439525101331 Published online by Cambridge University Press

- The multiplicative units of $\mathbb{Z}[i]$ are $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
- If $x$ is a real number and $n$ is the integer such that $n \le x < n+1$, we write $\lfloor x \rfloor = n$ and $\lceil x \rceil = n+1$. We also use the nearest integer function, given by

$$\lfloor x \rceil = \begin{cases} \lfloor x \rfloor & \text{if } 0 \le x - \lfloor x \rfloor \le 1/2 \\ \lceil x \rceil & \text{otherwise.} \end{cases}$$

- The minimal Euclidean function on a domain $R$ is $\phi_R$. We calculate $\phi_{\mathbb{Z}[i]}$ using the formula in Theorem 1.5; $\phi_{\mathbb{Z}[i]}(x)$ computes the length of $x$'s $(1+i)$-ary expansion.

### 1.1.2 Definitions

***Definition 1.1*** We define the sequence $w_m = \begin{cases} 3 \cdot 2^k & \text{if } m = 2k \\ 4 \cdot 2^k & \text{if } m = 2k+1. \end{cases}$

We repeatedly use that $w_{m+2} = 2w_m$ and that if $2^l < w_n$, then $2^l | w_m$ for all $m > n$. Note that if $2^l < w_n$ and $2^l \nmid w_n$, then $w_n = 3 \cdot 2^{l-1}$.

***Example 1.1*** The sequence begins with $w_0 = 3$, $w_1 = 4$, $w_2 = 6$, $w_3 = 8$, $w_4 = 12$, $w_5 = 16$, etc.

***Definition 1.2*** The function $m(z) = \ell_1(z) - \ell_\infty(z)$ is the minimum of the absolute values of the real and imaginary parts of $z$.

***Example 1.2*** We see $m(7-2i) = 2$, $m(1+i) = 1$, and $m(7) = m(7i) = 0$.

***Definition 1.3*** If $z \in \mathbb{C} \backslash \mathbb{Z}\{1 \pm i\}$, denote the unique unit such that $\mathrm{Re}(u_z z) = \ell_\infty(z)$ by $u_z$. If $z \in \mathbb{Z}\{1 \pm i\} \backslash \{0\}$, $u_z$ is the unique unit such that $u_z z = \ell_\infty(z)(1+i)$.

***Example 1.3*** Note $u_{2+i} = 1$, $u_{1-i} = i$, and $u_{-3+5i} = -i$.

***Definition 1.4*** For $r \in \mathbb{C}$, we define $s(r) = \mathrm{sgn}(\mathrm{Im}(u_r r))$.

***Example 1.4*** If $r = -3+5i$, $s(r) = \mathrm{sgn}(\mathrm{Im}(-i(-3+5i))) = \mathrm{sgn}(\mathrm{Im}(5+3i)) = \mathrm{sgn}(3) = 1$.

### 1.1.3 Background

Complex conjugation is multiplicative, so that $\overline{xy} = \overline{x} \cdot \overline{y}$, and hence the norm is also multiplicative. In other words, if $a, b \in \mathbb{Q}(i)$, then $\mathrm{Nm}(ab) = \mathrm{Nm}(a)\mathrm{Nm}(b)$. The Gaussians' multiplicative units, $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, have norm one and the set is closed under complex conjugation, so both the norm and $\phi_{\mathbb{Z}[i]}$ are invariant under complex conjugation and multiplication by units. If $u \in \mathbb{Z}[i]^\times$ and $z \in \mathbb{Z}[i] \backslash \{0\}$, then $\mathrm{Nm}(z) = \mathrm{Nm}(\overline{z}) = \mathrm{Nm}(uz)$ and $\phi_{\mathbb{Z}[i]}(z) = \phi_{\mathbb{Z}[i]}(\overline{z}) = \phi_{\mathbb{Z}[i]}(uz)$.

https://doi.org/10.4153/S0008439525101331 Published online by Cambridge University Press

## 1.2 Using the minimal Euclidean function on $\mathbb{Z}[i]$

Here, we present the formula for $\phi_{\mathbb{Z}[i]}$, and a division algorithm on $\mathbb{Z}[i]$ using $\phi_{\mathbb{Z}[i]}$.

***Theorem 1.5*** (Graves [1]) *Given $x + yi \in \mathbb{Z}[i]\backslash\{0\}$, let $j = v_2(\gcd(x, y))$ and $n$ be the smallest integer such that $\max\left(\frac{|x|}{2^j}, \frac{|y|}{2^j}\right) \leq w_n - 2$. If $\frac{|x|+|y|}{2^j} \leq w_{n+1} - 3$, then $\phi_{Z[i]}(x + yi) = n + 2j$. Otherwise, $\phi_{\mathbb{Z}[i]}(x + yi) = n + 2j + 1$.*

Thus, if $x$ and $y$ are $N$-bit integers, we can compute both $\phi_{\mathbb{Z}[i]}(x + yi)$ and one of $x + yi$'s minimal $(1 + i)$-ary expansions in $O(\log N)$ time, as shown in Section 4 of [1].

***Corollary 1.6*** (of Theorem 1.5) *If $z \in \mathbb{Z}[i]\backslash\{0\}$, if $\ell_\infty(z) \leq w_n - 2^{v_2(z)+1}$, and if $\ell_1(z) \leq w_{n+1} - 3 \cdot 2^{v_2(z)}$, then $\phi_{\mathbb{Z}[i]}(z) \leq n$. Note $\phi_{\mathbb{Z}[i]}(z) > n$ if and only if either $\ell_\infty(z) > w_n - 2^{v_2(z)+1}$ or $\ell_1(z) > w_{n+1} - 3 \cdot 2^{v_2(z)}$.*

Given $a, b \in \mathbb{Z}[i]\backslash\{0\}$, Theorem 1.7 below shows how to adjust the Gauss quotient and the Gauss remainder of $a$ and $b$ to find new quotients and remainders $q, r \in \mathbb{Z}[i]$ such that $a = qb + r$, where either $r = 0$ or $\phi_{\mathbb{Z}[i]}(r) < \phi_{\mathbb{Z}[i]}(b)$. Interestingly, there are times we do not have to compute the Gauss remainder to know whether we need to adapt it for $\phi_{\mathbb{Z}[i]}$.

***Theorem 1.7*** *Suppose $a, b \in \mathbb{Z}[i]\backslash\{0\}$ have Gauss remainder $r \neq 0$ with $\phi_{\mathbb{Z}[i]}(r) \geq \phi_{\mathbb{Z}[i]}(b) = n$ and $a = qb + r$. Consider the following conditions:*

(1) $2^{v_2(r)} \nmid w_{n-1}$.
(2) $\mathrm{Im}(u_b b)\mathrm{Im}(u_r r) \geq 0$.
(3) $m(r) + m(b) \leq \ell_\infty(r)$.
(4) $m(b) < \ell_\infty(r) < m(b) + m(r)$ *and* $\ell_\infty(b) - m(r) > w_{n-1} - 2^{v_2(b)+1}$.

*If any of the conditions hold, then $a = \left(q + \frac{u_b}{u_r}\right) b + \left(r - \frac{u_b}{u_r} b\right)$, with $\phi_{\mathbb{Z}[i]}\left(r - \frac{u_b}{u_r} b\right) < \phi_{\mathbb{Z}[i]}(b)$. If none hold, then $a = \left(q + \frac{iu_b}{s(r)u_r}\right) b + \left(r - \frac{iu_b}{s(r)u_r} b\right)$, with $\phi_{\mathbb{Z}[i]}\left(r - \frac{iu_b}{s(r)u_r} b\right) < \phi_{\mathbb{Z}[i]}(b)$.*

The rest of the article builds the machinery to prove Theorem 1.7. Section 2 presents the standard division algorithm.

Note that while Theorem 1.7 gives an algorithm to find a quotient and remainder using the minimal Euclidean function, the quotient and remainder are not necessarily unique. The two expansions in Equation (1.1) give two different quotient and remainder pairs with respect to the Gaussian's minimal Euclidean function for $2 + i$ and $1 + i$, $(2, -i)$ and $(1, 1)$.

It also constructs and presents properties of the ensuing (Gauss) remainder for $a, b \in \mathbb{Z}[i]$. Section 3 shows that if $v_2(r) \leq v_2(b)$, then $\phi_{\mathbb{Z}[i]}(r) < \phi_{\mathbb{Z}[i]}(b)$. Section 4 presents two possible alternate remainders for when $\phi_{\mathbb{Z}[i]}(r) \geq \phi_{\mathbb{Z}[i]}(b)$: $r - \frac{u_b}{u_r} b$ and $r - \frac{iu_b}{s(r)u_r} b$. Both sections introduce properties of $r$ and $b$ when $\phi_{\mathbb{Z}[i]}(r) \geq \phi_{\mathbb{Z}[i]}(b)$.

https://doi.org/10.4153/S0008439525101331 Published online by Cambridge University Press

Lemma 5.1 shows the absolute values of the real and imaginary parts of the alternate remainders are, respectively, elements of

$$\{|\ell_\infty(b) - \ell_\infty(r)|, m(b) + m(r)\} \text{ and } \{\ell_\infty(b) - m(r), |\ell_\infty(r) - m(b)|\}. \tag{1.2}$$

We therefore use the bounds on $\ell_\infty(r)$, $\ell_1(r)$, $m(r)$, and $\ell_\infty(b) - \ell_\infty(r)$ calculated in Section 4 to bound the sums and differences in (1.2). Lemma 4.6, Proposition 4.12, and Section 5's lemmas each assume one of the conditions in Theorem 1.7. They appropriately bound a subset of Equation (1.2)'s terms to prove which alternative remainder $x$ satisfies $\phi_{\mathbb{Z}[i]}(x) < \phi_{\mathbb{Z}[i]}(b)$. Every proposition and lemma cited in Theorem 1.7's proof is followed by an example illustrating our division algorithm in the corresponding scenario.

## 2 The standard division algorithm

Suppose $a, b \in \mathbb{Z}[i]\backslash\{0\}$, with $a = x + yi$ and $b = c + di$. Then, $\frac{a}{b}$ equals

$$\frac{a\overline{b}}{b\overline{b}} = \frac{a\overline{b}}{\mathrm{Nm}(b)} = \frac{(xc + yd) + (yc - xd)i}{\mathrm{Nm}(b)}.$$

If $q_0 = \left\lfloor \frac{xc+yd}{\mathrm{Nm}(b)} \right\rceil$, $q_1 = \left\lfloor \frac{yc-xd}{\mathrm{Nm}(b)} \right\rceil$, $f_0 = \frac{xc+yd}{\mathrm{Nm}(b)} - q_0$, and $f_1 = \frac{yc-xd}{\mathrm{Nm}(b)} - q_1$, then

$$\frac{a\overline{b}}{\mathrm{Nm}(b)} = (q_0 + q_1 i) + (f_0 + f_1 i), \text{ where } |f_0|, |f_1| \le \frac{1}{2}.$$

Multiplying through by $b$ shows

$$a = (q_0 + q_1 i)b + (f_0 + f_1 i)b, \tag{2.1}$$

where $q_0 + q_1 i, (f_0 + f_1 i)b \in \mathbb{Z}[i]$. The norm is multiplicative, so

$$\mathrm{Nm}(r) = \mathrm{Nm}((f_0 + f_1 i)b) = \mathrm{Nm}(f_0 + f_1 i)\mathrm{Nm}(b) \le \left(\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2\right)\mathrm{Nm}(b) \le \frac{\mathrm{Nm}(b)}{2}. \tag{2.2}$$

We call $f_0 + f_1 i$ the *Gauss fractional remainder of a and b* and $(f_0 + f_1 i)b$ the *Gauss remainder of a and b*.

***Example 2.1*** When $a = 7 + 5i$ and $b = 5 + 3i$,

$$\frac{a\overline{b}}{\mathrm{Nm}(b)} = \frac{(7 + 5i)(5 - 3i)}{5^2 + 3^2} = \frac{50 + 4i}{34} = 1 + \frac{8 + 2i}{17},$$

so the Gauss fractional remainder of $a$ and $b$ is $\frac{8+2i}{17}$. We see $a = 1 \cdot b + r$, where

$$r = \left(\frac{8 + 2i}{17}\right)(5 + 3i) = 2 + 2i.$$

***Lemma 2.2*** *Suppose $a, b, z \in \mathbb{Z}[i]\backslash\{0\}$. The pair a and b have Gauss remainder r if and only if za and zb have Gauss remainder zr.*

https://doi.org/10.4153/S0008439525101331 Published online by Cambridge University Press

**Proof** The fraction $\frac{za}{zb} \cdot \frac{\overline{zb}}{\overline{zb}}$ simplifies to $\frac{a}{b}$, so $za$ and $zb$ have the same Gauss fractional remainder as $a$ and $b$. This means that the Gauss remainder of $za$ and $zb$ is $za - qzb = zr$, or $z$ times the Gauss remainder of $a$ and $b$. ∎

***Example 2.3*** Continuing Example 2.1, $2 + 12i = (7 + 5i)(1 + i)$ and $2 + 8i = (5 + 3i)(1 + i)$ have Gauss remainder $4i = (2 + 2i)(1 + i)$.

***Lemma 2.4*** *If $a, b \in \mathbb{Z}[i]\backslash\{0\}$ have Gauss remainder $r \neq 0$ and if $\phi_{\mathbb{Z}[i]}(b) = n$, then $\ell_1(r) \leq \ell_\infty(b) < w_n$ and $\ell_\infty(r) \leq \frac{\ell_1(b)}{2} < w_{n-1}$. Equality occurs only if $\frac{r}{b} \in \left\{\pm\frac{1}{2}, \pm\frac{i}{2}, \pm\frac{1}{2} \pm \frac{i}{2}\right\}$.*

**Proof** For expositional ease, let $b = x + yi$ and denote the Gauss fractional remainder by $f_0 + f_1 i$. Equation (2.1) shows $r = (xf_0 - yf_1) + (xf_1 + yf_0)i$, so

$$\ell_\infty(r) = \max(|xf_0 - yf_1|, |xf_1 + yf_0|) \leq \frac{\ell_1(b)}{2} < \frac{w_{n+1}}{2} = w_{n-1} \tag{2.3}$$

and

$$\begin{aligned} \ell_1(r) &= \max(|xf_0 - yf_1 + xf_1 + yf_0|, |yf_1 - xf_0 + xf_1 + yf_0|) \\ &= \max(|f_0(x + y) + f_1(x - y)|, |f_0(y - x) + f_1(x + y)|) \\ &\leq \frac{\ell_1(b)}{2} + \frac{\ell_\infty(b) - m(b)}{2} = \ell_\infty(b) < w_n. \end{aligned} \tag{2.4}$$

Inequalities (2.3) and (2.4) are strict, unless $f_0, f_1 \in \left\{0, \pm\frac{1}{2}\right\}$. ∎

***Corollary 2.5*** *If $a, b \in \mathbb{Z}[i]\backslash\{0\}$ have Gauss remainder $r \neq 0$ and $\phi_{\mathbb{Z}[i]}(r) \geq \phi_{\mathbb{Z}[i]}(b)$, then $\ell_\infty(r) < \frac{\ell_1(b)}{2}$ and $\ell_1(r) < \ell_\infty(b)$.*

**Proof** If $f_0, f_1 \in \left\{0, \frac{1}{2}\right\}$, then $\frac{r}{b} \in (\mathbb{Z}[i]^\times)\{(1 + i)^{-1}, (1 + i)^{-2}\}$ and $\phi_{\mathbb{Z}[i]}(r) \in \{\phi_{\mathbb{Z}[i]}(b) - 1, \phi_{\mathbb{Z}[i]}(b) - 2\}$. Thus, $\phi_{\mathbb{Z}[i]}(r) \geq \phi_{\mathbb{Z}[i]}(b)$, our inequalities are strict. ∎

***Example 2.6*** Staying with Example 2.1, note $\phi_{\mathbb{Z}[i]}(b) = \phi_{\mathbb{Z}[i]}(r) = 3$, $\ell_1(r) = 4 < 5 = \ell_\infty(b) < 8 = w_3$, and $\ell_\infty(r) = 2 < \frac{\ell_1(b)}{2} = \frac{8}{2} = 4 < 6 = w_2$.

## 3 Gauss remainders and the minimal Euclidean function

Lemma 2.4 shows that if $a$ and $b$ have Gauss remainder $r$, $\phi_{\mathbb{Z}[i]}(r)$ is often less than $\phi_{\mathbb{Z}[i]}(b)$. Sometimes, we can determine whether $\phi_{\mathbb{Z}[i]}(r) < \phi_{\mathbb{Z}[i]}(b)$ without computing $r$.

***Lemma 3.1*** *If $a, b \in \mathbb{Z}[i]\backslash\{0\}$ have Gauss remainder $r \neq 0$ and $v_2(r) \leq v_2(b)$, then $\phi_{\mathbb{Z}[i]}(r) < \phi_{\mathbb{Z}[i]}(b) = n$.*

**Proof** If we assume either $\ell_1(r) = \ell_\infty(b)$ or $2\ell_\infty(r) = \ell_1(b)$, then Lemma 2.4 shows $\frac{r}{b} \in \pm\frac{1}{2}\{1, i, 1 \pm i\}$, and hence $\phi_{\mathbb{Z}[i]}(r) < \phi_{\mathbb{Z}[i]}(b)$. We therefore assume neither

https://doi.org/10.4153/S0008439525101331 Published online by Cambridge University Press

equality holds. Our hypothesis therefore implies

$$2^{v_2(r)} \le \ell_1(r) < \ell_\infty(b) \le w_n - 2^{v_2(b)+1} \le w_n - 2^{v_2(r)+1},$$

which leads to the observation $3 \cdot 2^{v_2(r)} < w_n$. Since $3 \cdot 2^{v_2(r)} \le w_n$, $2^{v_2(r)} | w_m$ for all $m \ge n$ and

$$\ell_1(r) \le w_n - 3 \cdot 2^{v_2(r)}.$$

Our hypothesis also implies

$$\ell_\infty(r) < \frac{\ell_1(b)}{2} \le \frac{w_{n+1} - 3 \cdot 2^{v_2(r)}}{2},$$

so $\ell_\infty(r) \le w_{n-1} - 2^{v_2(r)+1}$ and $\phi_{\mathbb{Z}[i]}(r) \le n - 1 < \phi_{\mathbb{Z}[i]}(b)$. ∎

***Corollary 3.2*** *If $a, b \in \mathbb{Z}[i]\backslash\{0\}$ have Gauss remainder $r \neq 0$ and $v_2(a) \le v_2(b)$, then $\phi_{\mathbb{Z}[i]}(r) < \phi_{\mathbb{Z}[i]}(b)$.*

***Example 3.3*** The Gauss remainder $r$ of $a = 9 + 4i$ and $b = 3 + 5i$ satisfies $\phi_{\mathbb{Z}[i]}(r) < \phi_{\mathbb{Z}[i]}(b)$ because 2 divides neither $a$ nor $b$.

***Corollary 3.4*** *If $a, b \in \mathbb{Z}[i]\backslash\{0\}$ have Gauss remainder $r \neq 0$ with $\phi_{\mathbb{Z}[i]}(r) \ge \phi_{\mathbb{Z}[i]}(b) = n$, then $2^{v_2(b)+1} | w_n$.*

**Proof** We prove the contrapositive and assume $2^{v_2(b)+1} \nmid w_n$. Jointly, our hypotheses and $2^{v_2(b)} \le \ell_\infty(b) \le w_n - 2^{v_2(b)+1}$ demonstrate $w_n = 3 \cdot 2^{v_2(b)}$. By Lemma 2.4, $2^{v_2(r)} \le \ell_1(r) < \ell_\infty(b) = 2^{v_2(b)}$. Lemma 3.1 then shows $\phi_{\mathbb{Z}[i]}(r) < \phi_{\mathbb{Z}[i]}(b)$. ∎

***Example 3.5*** Suppose $k = v_2(b)$ and $\phi_{\mathbb{Z}[i]}(b) = n$. The condition $2^{k+1} \nmid w_n$ holds if and only if $\ell_\infty(b) = 2^k$, $n = 2k$, and $m(b) = 0$. For all $a \in \mathbb{Z}[i]$, the Gauss remainder $r$ of $a$ and $2^k$ satisfies $\phi_{\mathbb{Z}[i]}(r) < \phi_{\mathbb{Z}[i]}(b)$.

## 4 Constructing alternate remainders

Example 4.1 shows that, unlike in Corollary 3.2, computing a remainder for $a, b \in \mathbb{Z}[i]\backslash\{0\}$ and $\phi_{\mathbb{Z}[i]}$ is not so simple when $v_2(r) > v_2(b)$. In this section, we construct alternate remainders, for when $\phi_{\mathbb{Z}[i]}(r) \ge \phi_{\mathbb{Z}[i]}(b)$. The new remainder determines the new quotient. If $R$ is the new remainder, then the associated quotient is the integer $\frac{a-R}{b}$.

***Example 4.1*** Observe $v_2(4 + i) = 0$, $\phi_{\mathbb{Z}[i]}(2i) = 2 = \phi_{\mathbb{Z}[i]}(4 + i)$, and that the Gauss remainder of 9 and $4 + i$ is $2i$, so $2i$ is not the pair's remainder for $\phi_{\mathbb{Z}[i]}$.

### 4.1 Valuations and preliminaries

***Lemma 4.2*** *If $\phi_{\mathbb{Z}[i]}(b) = n > 0$, then $m(b) \le w_{n-1} - 2^{v_2(b)+1}$.*

https://doi.org/10.4153/S0008439525101331 Published online by Cambridge University Press

**Proof** Since $2^{v_2(b)} \le w_n - 2^{v_2(b)+1}$, $3 \cdot 2^{v_2(b)} \le w_n$, and $2^{v_2(b)+1} | w_m$ for all $m \ge n+1$. The bound

$$2m(b) \le \ell_1(b) \le w_{n+1} - 3 \cdot 2^{v_2(b)}$$

therefore implies

$$2m(b) \le w_{n+1} - 4 \cdot 2^{v_2(b)}.$$

Dividing by two finishes the proof. ∎

***Example 4.3*** If $b = 5 + 3i$, $\phi_{\mathbb{Z}[i]}(b) = 3$, $v_2(b) = 0$, $w_2 = 6$, and $m(b) = 3 < 6 - 2 = 4$.

***Lemma 4.4*** *If $a, b \in \mathbb{Z}[i] \backslash \{0\}$ have Gauss remainder $r \neq 0$ and $\phi_{\mathbb{Z}[i]}(r) \ge \phi_{\mathbb{Z}[i]}(b) = n$, then $\ell_\infty(b) - m(b) \le w_n - 3 \cdot 2^{v_2(b)}$.*

**Proof** If $m(b) > 0$, then

$$\ell_\infty(b) - m(b) \le w_n - 2^{v_2(b)+1} - 2^{v_2(b)} = w_n - 3 \cdot 2^{v_2(b)}$$

by Theorem 1.5. Corollary 3.4 states $2^{v_2(b)+1} | w_n$, so $2^{v_2(b)+1} | (w_n - 2^{v_2(b)+1})$. When $m(b) = 0$, we see $2^{v_2(b)+1} \nmid \ell_\infty(b)$. Theorem 1.5 therefore implies

$$\ell_\infty(b) - m(b) = \ell_\infty(b) < w_n - 2^{v_2(b)+1}. \tag{4.1}$$

Since $2^{v_2(b)}$ divides all terms in Equation (4.1), our claim follows. ∎

***Example 4.5*** The pair $a = 21 + 8i$ and $b = 13 + 8i$ have Gauss remainder $r = 8$, and $\phi_{\mathbb{Z}[i]}(8) = 6 > 5 = \phi_{\mathbb{Z}[i]}(13 + 8i)$. Observe $2^{v_2(b)} = 2$, $w_5 = 16$, and

$$\ell_\infty(b) - m(b) = 13 - 8 = 5 < 16 - 3.$$

***Lemma 4.6*** *Suppose $a, b \in \mathbb{Z}[i] \backslash \{0\}$ have Gauss remainder $r \neq 0$ with $\phi_{\mathbb{Z}[i]}(r) \ge \phi_{\mathbb{Z}[i]}(b) = n$. If $2^{v_2(r)} \nmid w_{n-1}$, then $m(r) = 0$. Furthermore, $\phi_{\mathbb{Z}[i]}\left(r - \frac{u_b}{u_r} b\right) < \phi_{\mathbb{Z}[i]}(b)$.*

**Proof** Since Lemma 2.4 shows $2^{v_2(r)} \le \ell_\infty(r) \le \frac{\ell_1(b)}{2} < w_{n-1}$, our hypothesis implies $w_n = 2^{v_2(r)+1}$ and thus

$$2^{v_2(r)} \le \ell_\infty(r) \le \ell_1(r) < \ell_\infty(b) < w_n = 2^{v_2(r)+1}.$$

We infer $\ell_\infty(r) = \ell_1(r)$, $m(r) = 0$, and $u_b b - u_r r \in \{(\ell_\infty(b) - \ell_\infty(r)) \pm m(b) i\}$. Lemma 4.2 shows

$$\begin{aligned} \ell_\infty(u_b b - u_r r) &\le \max(\ell_\infty(b) - \ell_\infty(r), m(b)) \\ &\le (w_n - 2^{v_2(b)+1} - 2^{v_2(r)}, w_{n-1} - 2^{v_2(b)+1}) \\ &\le w_{n-1} - 2^{v_2(b)+1}; \end{aligned}$$

https://doi.org/10.4153/S0008439525101331 Published online by Cambridge University Press

we observe

$$\begin{aligned}\ell_1(u_b b - u_r r) &= \ell_1(b) - \ell_\infty(r)\\ &\le w_{n+1} - 3\cdot 2^{v_2(b)} - 2^{v_2(r)}\\ &= w_n - 3\cdot 2^{v_2(b)}.\end{aligned}$$

As $v_2(u_b b - u_r r) = v_2(b)$, $\phi_{\mathbb{Z}[i]}\left(r - \frac{u_b}{u_r} b\right) = \phi_{\mathbb{Z}[i]}(u_b b - u_r r) < \phi_{\mathbb{Z}[i]}(b)$. ∎

***Example 4.7*** Continuing Example 4.5, recall $\phi_{\mathbb{Z}[i]}(b) = 5 < 6 = \phi_{\mathbb{Z}[i]}(r)$. We see $u_b b - u_r r = (13 + 8i) - 8 = 5 + 8i$ and $\phi_{\mathbb{Z}[i]}(5 + 8i) = 4 < 5 = \phi_{\mathbb{Z}[i]}(b)$.

Since we understand what happens when $\phi_{\mathbb{Z}[i]}(r) \ge \phi_{\mathbb{Z}[i]}(b)$ and $2^{v_2(r)} \nmid w_{n-1}$, we study when $2^{v_2(r)} | w_{n-1}$.

***Lemma 4.8*** *Suppose $a, b \in \mathbb{Z}[i]\backslash\{0\}$ have Gauss remainder $r \neq 0$, where $\phi_{\mathbb{Z}[i]}(r) \ge \phi_{\mathbb{Z}[i]}(b) = n$. If $2^{v_2(r)} | w_{n-1}$, then $2^{v_2(r)} | w_m$ for all $m \ge n-1$ and either*

$$\ell_\infty(r) = w_{n-1} - 2^{v_2(r)} \text{ or } \ell_1(r) \ge w_n - 2^{v_2(r)+1}.$$

*In both cases,*

$$\ell_\infty(r) \ge w_n - w_{n-1} \text{ and } \ell_1(r) \ge w_{n-1} - 2^{v_2(r)}.$$

*If $\ell_\infty(r) \neq w_{n-1} - 2^{v_2(r)}$, then $m(r) \ge w_n - w_{n-1}$.*

**Proof** The first line of Lemma 4.6's proof shows $2^{v_2(r)} \le \ell_\infty(r) < w_{n-1}$, so $\ell_\infty(r) \le w_{n-1} - 2^{v_2(r)}$. Since $2^{v_2(r)+1} \le w_{n-1}$, Definition 1.1 shows $2^{v_2(r)} | w_m$ for all $m \ge n-1$. Our assumption that $\phi_{\mathbb{Z}[i]}(r) > n-1$ and Corollary 1.6 show either $\ell_\infty(r) = w_{n-1} - 2^{v_2(r)}$ or $\ell_1(r) \ge w_n - 2^{v_2(r)+1}$. Since $\ell_1(r) \ge \ell_\infty(r)$ and $w_n - 2^{v_2(r)+1} \ge w_{n-1} - 2^{v_2(r)}$, we see that in both cases, $\ell_1(r) \ge w_{n-1} - 2^{v_2(r)}$.

If $\ell_{\infty(r)} \le w_{n-1} - 2^{v_2(r)+1}$, then $\ell_1(r) = \ell_\infty(r) + m(r) \ge w_n - 2^{v_2(r)+1}$ implies

$$m(r) \ge w_n - 2^{v_2(r)+1} - (w_{n-1} - 2^{v_2(r)+1}) = w_n - w_{n-1}.$$

In both cases, $\ell_\infty(r) \ge w_n - w_{n-1}$, as $\ell_\infty(r) \ge \min(m(r), w_{n-1} - 2^{v_2(r)})$ and

$$2(w_{n-1}) - 2^{v_2(r)} = w_{n+1} - 2^{v_2(r)} \ge w_n.$$ ∎

***Example 4.9*** In Example 2.1, $\phi_{\mathbb{Z}[i]}(r) = \phi_{\mathbb{Z}[i]}(b) = 3$. Note $2^{v_2(r)} = 2$ divides $w_2 = 6$ and all $w_m$, $m \ge 2$. We see $\ell_\infty(r) = 2 = w_2 - 2^{v_2(r)}$ and $\ell_1(r) = 4 > w_3 - 2^{v_2(r)+1} = 8 - 8 = 0$, so our example is in both of Lemma 4.8's (non-exclusive) scenarios. We see $\ell_\infty(r) = m(r) = 2 = w_3 - w_2$ and $\ell_1(r) = 4 > w_2 - 2^{v_2(r)} = 6 - 4 = 2$.

***Corollary 4.10*** *Suppose $a, b \in \mathbb{Z}[i]\backslash\{0\}$ have Gauss remainder $r \neq 0$, with $\phi_{\mathbb{Z}[i]}(r) \ge \phi_{\mathbb{Z}[i]}(b) = n$. If $2^{v_2(r)} | w_{n-1}$, then $m(r)$, $\ell_\infty(r)$, and $\ell_\infty(b) - \ell_\infty(r) \le w_{n-1} - 2^{v_2(b)+1}$.*

https://doi.org/10.4153/S0008439525101331 Published online by Cambridge University Press

**Proof** Lemma 3.1 shows $v_2(r) > v_2(b)$, so

$$m(r) \le \ell_\infty(r) \le w_{n-1} - 2^{v_2(r)} \le w_{n-1} - 2^{v_2(b)+1}.$$

By Lemma 4.8,

$$\ell_\infty(b) - \ell_\infty(r) \le (w_n - 2^{v_2(b)+1}) - (w_n - w_{n-1}) = w_{n-1} - 2^{v_2(b)+1}. \qquad \blacksquare$$

***Example 4.11*** Continuing Example 2.1, we see $m(r) = \ell_\infty(r) = 2$ and $\ell_\infty(b) - \ell_\infty(r) = 5 - 2 = 3$ are both less than $w_2 - 2^{v_2(b)+1} = 6 - 2 = 4$.

### 4.2 When imaginary parts align

Determining an alternate remainder is fairly straightforward when $\mathrm{Im}(u_b b)\mathrm{Im}(u_r r) \ge 0$, i.e., when $u_b b$ and $u_r r$ lie in the same quadrant. They lie in the same quadrant, and not just the same half-plane, because Definition 1.3 ensures $\mathrm{Re}(u_b b), \mathrm{Re}(u_r r) \ge 0$. The next section shows things become much more complicated when $u_b b$ and $u_r r$ lie in different quadrants.

***Proposition 4.12*** *Suppose $a, b \in \mathbb{Z}[i]\backslash\{0\}$ have Gauss remainder $r \neq 0$ with $\phi_{\mathbb{Z}[i]}(r) \ge \phi_{\mathbb{Z}[i]}(b) = n$. If $\mathrm{Im}(u_b b)\mathrm{Im}(u_r r) \ge 0$, then $\phi_{\mathbb{Z}[i]}\left(r - \frac{u_b}{u_r} b\right) < \phi_{\mathbb{Z}[i]}(b)$.*

**Proof** Lemma 4.6 lets us assume that $2^{v_2(r)} | w_m$ for all $m \ge n-1$. Since

$$u_b b - u_r r \in \{(\ell_\infty(b) - \ell_\infty(r)) \pm (m(b) - m(r))i\},$$

Corollary 4.10 shows

$$\ell_\infty(u_b b - u_r r) \le \max(\ell_\infty(b) - \ell_\infty(r), m(b), m(r)) \le w_{n-1} - 2^{v_2(b)+1}.$$

Observe that, due to Lemmas 4.4 and 4.8,

$$\begin{aligned}
\ell_1(u_b b - u_r r) &= \max(\ell_1(b) - \ell_1(r), \ell_\infty(b) - m(b) + m(r) - \ell_\infty(r)) \\
&\le \max(w_{n+1} - 3 \cdot 2^{v_2(b)} - (w_{n-1} - 2^{v_2(r)}), \ell_\infty(b) - m(b)) \\
&\le \max(w_{n-1} + 2^{v_2(r)} - 3 \cdot 2^{v_2(b)}, w_n - 3 \cdot 2^{v_2(b)}) \\
&\le w_n - 3 \cdot 2^{v_2(b)}.
\end{aligned}$$

Lemma 3.1 shows $v_2(u_b b - u_r r) = v_2(b)$ and thus $\phi_{\mathbb{Z}[i]}\left(r - \frac{u_b}{u_r} b\right) = \phi_{\mathbb{Z}[i]}(u_b b - u_r r) < \phi_{\mathbb{Z}[i]}(b)$. $\blacksquare$

***Example 4.13*** Continuing Example 2.1, note $\mathrm{Im}(u_b b)\mathrm{Im}(u_r r) = 3 \cdot 2 = 6 > 0$ and $\phi_{\mathbb{Z}[i]}(u_b b - u_r r) = \phi_{\mathbb{Z}[i]}(3 + i) = 2 < 3 = \phi_{\mathbb{Z}[i]}(b) = \phi_{\mathbb{Z}[i]}(r)$.

## 5 Proving our main result

When $\mathrm{Im}(u_b b)$ and $\mathrm{Im}(u_r r)$ have opposite signs, finding alternate remainders becomes more complicated. It only partially depends on how $r$ relates to $m(b)$.

https://doi.org/10.4153/S0008439525101331 Published online by Cambridge University Press

In this section, we construct alternate remainders for when $\phi_{\mathbb{Z}[i]}(r) \geq \phi_{\mathbb{Z}[i]}(b)$ and $\mathrm{Im}(u_b b)\mathrm{Im}(u_r r) < 0$, allowing us to prove Theorem 1.7.

***Lemma 5.1*** *Suppose $a, b \in \mathbb{Z}[i]\backslash\{0\}$ have Gauss remainder $r \neq 0$ with $\phi_{\mathbb{Z}[i]}(r) \geq \phi_{\mathbb{Z}[i]}(b) = n$. If $\mathrm{Im}(u_b b)\mathrm{Im}(u_r r) < 0$, then*

$$u_b b - u_r r \in \{(\ell_\infty(b) - \ell_\infty(r)) \pm (m(b) + m(r))i\}$$

*and*

$$u_b b + s(r) i u_r r \in \{(\ell_\infty(b) - m(r)) \pm (m(b) - \ell_\infty(r))i\}.$$

**Proof** The first equation follows from the definitions. The assumption $\mathrm{Im}(u_b b)\mathrm{Im}(u_r r) < 0$ implies that if $u_b b = \ell_\infty(b) \pm m(b)i$, then $u_r r = \ell_\infty(r) \mp m(r)i$ and $iu_r r = \pm m(r) + \ell_\infty(r)i$. Since $s(r) = \mathrm{sgn}(\mathrm{Im}(u_r r))$, $s(r) i u_r r = -m(r) \mp \ell_\infty(r)i$. We conclude that $u_b b + s(r) i u_r r = (\ell_\infty(b) - m(r)) \pm (m(b) - \ell_\infty(r))i$. ∎

***Example 5.2*** The Gauss remainder of $a = 16 + i$ and $b = 10 + 3i$ is $r = 6 - 2i$, with $\phi_{\mathbb{Z}[i]}(b) = \phi_{\mathbb{Z}[i]}(r) = 4$ and $\mathrm{Im}(b)\mathrm{Im}(r) = -6 < 0$. We see

$$u_b b - u_r r = (10 + 3i) - (6 - 2i) = 4 + 5i = (\ell_\infty(b) - \ell_\infty(r)) + (m(b) + m(r))i$$

and

$$u_b b + s(r) i u_r r = (10 + 3i) - i(6 - 2i) = 8 - 3i = (\ell_\infty(b) - m(r)) + (m(b) - \ell_\infty(r))i.$$

***Lemma 5.3*** *Suppose $a, b \in \mathbb{Z}[i]\backslash\{0\}$ have Gauss remainder $r \neq 0$ with $\phi_{\mathbb{Z}[i]}(r) \geq \phi_{\mathbb{Z}[i]}(b) = n$. If $\mathrm{Im}(u_b b)\mathrm{Im}(u_r r) < 0$ and $m(b) \geq \ell_\infty(r)$, then $\phi_{\mathbb{Z}[i]}\left(r - \frac{u_b i}{s(r) u_r} b\right) < \phi_{\mathbb{Z}[i]}(b)$.*

**Proof** Harken back to Lemma 3.1 and observe $v_2(b) = v_2(u_b b + s(r) i u_r r)$. Since $m(b) \geq \ell_\infty(r)$, Lemma 5.1 shows

$$\ell_1(u_b b + s(r) i u_r r) = \ell_1(b) - \ell_1(r). \tag{5.1}$$

Our assumption $\mathrm{Im}(u_b b)\mathrm{Im}(u_r r) < 0$ implies $m(r) \neq 0$. If $\ell_\infty(r) = w_{n-1} - 2^{v_2(r)}$, then

$$\ell_1(r) = \ell_\infty(r) + m(r) \geq (w_{n-1} - 2^{v_2(r)}) + 2^{v_2(r)} = w_{n-1}.$$

Equation (5.1) then shows

$$\ell_1(u_b b + s(r) i u_r r) \leq w_{n+1} - 3 \cdot 2^{v_2(b)} - w_{n-1} = w_{n-1} - 3 \cdot 2^{v_2(b)},$$

demonstrating $\phi_{\mathbb{Z}[i]}(u_b b + s(r) i u_r r) \leq n - 1$.

If $\ell_\infty(r) \neq w_{n-1} - 2^{v_2(r)}$, Lemmas 4.6 and 4.8 show $\ell_1(r) \geq w_n - 2^{v_2(r)+1}$ and $2^{v_2(r)+1}$ divides both $w_{n+1}$ and $w_{n+2}$. This means $2^{v_2(r)+1} \leq w_{n+2} - w_{n+1}$, so $\ell_1(r) \geq w_{n+1} - w_n$. We deduce from Equation (5.1) that

$$\ell_1(u_b b + s(r) i u_r r) \leq (w_{n+1} - 3 \cdot 2^{v_2(b)}) - (w_{n+1} - w_n) = w_n - 3 \cdot 2^{v_2(b)}.$$

https://doi.org/10.4153/S0008439525101331 Published online by Cambridge University Press

Corollary 4.10 and Lemma 5.1 show

$$\ell_\infty(u_b b + s(r) i u_r r) \le \max(\ell_\infty(b) - m(r), m(b), \ell_\infty(r)) \le w_{n-1} - 2^{v_2(b)+1},$$

proving $\phi_{\mathbb{Z}[i]}\left(r - \frac{iu_b}{s(r)u_r} b\right) = \phi_{\mathbb{Z}[i]}(u_b b + s(r) i u_r r) < \phi_{\mathbb{Z}[i]}(b)$. ∎

***Example 5.4*** The Gauss remainder of $a = 8 + 8i$ and $b = 30 - 9i$ is $r = 8 + 8i$, and thus $u_b b + s(r) i u_r r = (30 - 9i) + i(8 + 8i) = 22 - i$. Note $\phi_{\mathbb{Z}[i]}(b) = \phi_{\mathbb{Z}[i]}(r) = 7$, $\mathrm{Im}(u_b b)\mathrm{Im}(u_r r) = -72 < 0$, and $\phi_{\mathbb{Z}[i]}(22 - i) = 6 < \phi_{\mathbb{Z}[i]}(b)$.

***Lemma 5.5*** *Suppose $a, b \in \mathbb{Z}[i]\backslash\{0\}$ have Gauss remainder $r \neq 0$ with $\phi_{\mathbb{Z}[i]}(r) \ge \phi_{\mathbb{Z}[i]}(b) = n$. If $\mathrm{Im}(u_b b)\mathrm{Im}(u_r r) < 0$ and $m(r) + m(b) \le \ell_\infty(r)$, then $\phi_{\mathbb{Z}[i]}\left(r - \frac{u_b}{u_r} b\right) < \phi_{\mathbb{Z}[i]}(b)$.*

**Proof** Lemmas 3.1 and 4.8 show $v_2(r) > v_2(b) = v_2(u_b b - u_r r)$ and $2^{v_2(b)+1}$ divides $w_m$ for all $m \ge n + 1$. By Lemma 5.1 and Corollary 4.10,

$$\begin{aligned}\ell_\infty(u_b b - u_r r) &\le \max(\ell_\infty(b) - \ell_\infty(r), m(b) + m(r)) \\ &\le \max(\ell_\infty(b) - \ell_\infty(r), \ell_\infty(r)) \\ &\le w_{n-1} - 2^{v_2(b)+1}\end{aligned}$$

and

$$\ell_1(u_b b - u_r r) = \ell_\infty(b) - \ell_\infty(r) + m(b) + m(r).$$

If $\ell_\infty(r) > m(b) + m(r)$,

$$\ell_1(u_b b - u_r r) \le \ell_\infty(b) - 2^{v_2(r)} \le w_n - 3 \cdot 2^{v_2(r)}.$$

When $\ell_\infty(r) = m(r) + m(b)$, $2^{v_2(r)} | m(b)$ and thus $2^{v_2(b)+1} | m(b)$. Hence, $2^{v_2(b)+1} \nmid \ell_\infty(b)$ and, as $2^{v_2(b)+1} | (w_n - 2^{v_2(b)+1})$, $\ell_1(u_b b - u_r r) = \ell_\infty(b) \le w_n - 3 \cdot 2^{v_2(b)}$. We conclude $\phi_{\mathbb{Z}[i]}\left(r - \frac{u_b}{u_r} b\right) = \phi_{\mathbb{Z}[i]}(u_b b - u_r r) < \phi_{\mathbb{Z}[i]}(b)$. ∎

***Example 5.6*** In Example 5.2, we see $m(r) + m(b) = 5 < 6 = \ell_\infty(r)$, so

$$\phi_{\mathbb{Z}[i]}(u_b b - u_r r) = \phi_{\mathbb{Z}[i]}(4 + 5i) = 3 < \phi_{\mathbb{Z}[i]}(b) = 4.$$

We found alternate remainders when $\ell_\infty(r) \le m(b)$ and when $\ell_\infty(r) \ge m(b) + m(r)$, so we examine when $m(b) + m(r) > \ell_\infty(r) > m(b)$.

***Lemma 5.7*** *Suppose $a, b \in \mathbb{Z}[i]\backslash\{0\}$ have Gauss remainder $r \neq 0$ with $\phi_{\mathbb{Z}[i]}(r) \ge \phi_{\mathbb{Z}[i]}(b) = n$. If*

(1) $\mathrm{Im}(u_b b)\mathrm{Im}(u_r r) < 0$,
(2) $m(b) < \ell_\infty(r) < m(b) + m(r)$, *and*
(3) $\ell_\infty(b) - m(r) \le w_{n-1} - 2^{v_2(b)+1}$,

*then $\phi_{\mathbb{Z}[i]}\left(r - \frac{iu_b}{s(r)u_r} b\right) < \phi_{\mathbb{Z}[i]}(b)$.*

https://doi.org/10.4153/S0008439525101331 Published online by Cambridge University Press

**Proof** Lemma 3.1 shows $v_2(r) > v_2(b) = v_2(u_b b + s(r) i u_r r)$. By Lemma 5.1 and Corollary 4.10, we see

$$\ell_\infty(u_b b + s(r) i u_r r) \le \max(\ell_\infty(b) - m(r), \ell_\infty(r)) \le w_{n-1} - 2^{v_2(b)+1}$$

and

$$\ell_1(u_b b + s(r) i u_r r) = \ell_\infty(b) + (\ell_\infty(r) - (m(b) + m(r))) < w_n - 2^{v_2(b)+1}.$$

Lemma 4.8 shows $2^{v_2(b)} | w_n$, so $\ell_1(u_b b + s(r) i u_r r) \le w_n - 3 \cdot 2^{v_2(b)}$. We conclude that $\phi_{\mathbb{Z}[i]}\left(r - \frac{i u_b}{s(r) u_r} b\right) = \phi_{\mathbb{Z}[i]}(u_b b + s(r) i u_r r) < \phi_{\mathbb{Z}[i]}(b)$. ∎

***Example 5.8*** The Gauss remainder of $a = 16 - 8i$ and $b = 30 + 15i$ is $r = a$. Observe that $\phi_{\mathbb{Z}[i]}(16 - 8i) = \phi_{\mathbb{Z}[i]}(30 + 15i) = 7$, that $\mathrm{Im}(16 - 8i)\mathrm{Im}(30 + 15i) < 0$, that $15 < 16 < 8 + 15$, and that $30 - 8 = 22 = w_6 - 2$. As expected,

$$\phi_{\mathbb{Z}[i]}(u_b b + s(r) i u_r r) = \phi_{\mathbb{Z}[i]}(30 + 15i - (8 + 16i)) = \phi_{\mathbb{Z}[i]}(22 - i) = 6 < 7.$$

***Lemma 5.9*** *Suppose $a, b \in \mathbb{Z}[i] \backslash \{0\}$ have Gauss remainder $r \neq 0$ with $\phi_{\mathbb{Z}[i]}(r) \ge \phi_{\mathbb{Z}[i]}(b) = n$. If*

(1) $\mathrm{Im}(u_b b)\mathrm{Im}(u_r r) < 0$,
(2) $m(b) < \ell_\infty(r) < m(r) + m(b)$, *and*
(3) $\ell_\infty(b) - m(r) > w_{n-1} - 2^{v_2(b)+1}$,

*then* $\phi_{\mathbb{Z}[i]}\left(r - \frac{u_b}{u_r} b\right) < \phi_{\mathbb{Z}[i]}(b)$.

**Proof** For the last time, Lemmas 3.1 and 4.8 show that $2^{v_2(r)} | w_m$ for all $m \ge n - 1$ and $v_2(r) > v_2(b) = v_2(u_b b - u_r r)$. Condition (3) is equivalent to

$$\ell_\infty(b) - w_{n-1} + 2^{v_2(b)+1} > m(r). \tag{5.2}$$

Using $w_n - 2^{v_2(b)+1} \ge \ell_\infty(b)$ yields

$$w_n - w_{n-1} - 2^{v_2(r)} \ge m(r). \tag{5.3}$$

Adding $m(b)$ to both sides of Equation (5.2) and recalling $w_{n+1} - 3 \cdot 2^{v_2(b)} \ge \ell_1(b)$, we realize

$$w_{n-1} - 2^{v_2(b)+1} \ge m(b) + m(r). \tag{5.4}$$

Together, Equation (5.3) and Lemma 4.8 show that, as $m(r) < w_n - w_{n-1}$, $\ell_\infty(r) = w_{n-1} - 2^{v_2(r)}$. This equality, along with Lemma 5.1, Corollary 4.10, and Equations (5.3) and (5.4), demonstrates

$$\ell_\infty(u_b b - u_r r) \le \max(\ell_\infty(b) - \ell_\infty(r), m(b) + m(r)) \le w_{n-1} - 2^{v_2(b)+1}$$

and

$$\begin{aligned} \ell_1(u_b b - u_r r) &= \ell_\infty(b) + m(b) - \ell_\infty(r) + m(r) \\ &\le (w_{n+1} - 3 \cdot 2^{v_2(b)}) - (w_{n-1} - 2^{v_2(r)}) + (w_n - w_{n-1} - 2^{v_2(r)}) \\ &= w_n - 3 \cdot 2^{v_2(b)}. \end{aligned}$$

In summary, $\phi_{\mathbb{Z}[i]}\left(r - \frac{u_b}{u_r} b\right) = \phi_{\mathbb{Z}[i]}(u_b b - u_r r) < \phi_{\mathbb{Z}[i]}(b)$. ∎

https://doi.org/10.4153/S0008439525101331 Published online by Cambridge University Press

***Example 5.10*** The Gauss remainder of $a = 20 - 4i$ and $b = 28 + 17i$ is $r = a$. We see $\phi_{\mathbb{Z}[i]}(20 - 4i) = \phi_{\mathbb{Z}[i]}(28 + 17i) = 7$, $\mathrm{Im}(20 - 4i)\mathrm{Im}(28 + 17i) < 0$, $17 < 20 < 17 + 4$, and $28 - 4 = 24 > w_6 - 2$. As claimed,

$$\phi_{\mathbb{Z}[i]}(u_b b - u_r r) = \phi_{\mathbb{Z}[i]}(28 + 17i - (20 - 4i)) = \phi_{\mathbb{Z}[i]}(8 + 21i) = 6 < 7.$$

We now assemble our lemmas to prove Theorem 1.7.

**Proof** Proposition 4.12 proves our claim when condition 1 holds, Lemma 5.5 proves it when condition 2 holds, and Lemma 5.9 proves it when condition 3 holds.

If $\mathrm{Im}(u_b b)\mathrm{Im}(u_r r) < 0$ and neither condition 2 nor condition 3 hold, then either $m(b) \geq \ell_\infty(r)$ or $m(b) < \ell_\infty(r) < m(b) + m(r)$ and $\ell_\infty(b) - m(r) \leq w_{n-1} - 2^{v_2(b)+1}$. Lemmas 5.3 proves our theorem in the first situation, and Lemma 5.7 proves it in the second. ∎

**Acknowledgments** I thank my family for their patience with me when I had the key insight on our vacation, and Jon Grantham and Tad White for our fruitful discussions. Harold Conn and the article's referees provided valuable advice.

## References

[1] H. Graves, *The minimal Euclidean function on the Gaussian integers*. Indag. Math. (N.S.) **34**(2023), no. 1, 78–88. https://doi.org/10.1016/j.indag.2022.09.005
[2] H. W. Lenstra, Jr., *Lectures on Euclidean rings*. Bielefield. 1974. https://www.math.leidenuniv.nl/lenstrahw/PUBLICATIONS/1975b/art.pdf
[3] T. Motzkin, *The Euclidean algorithm*. Bull. Amer. Math. Soc **55**(1949), 1142–1146. https://doi.org/10.1090/s0002-9904-1949-09344-8

*IDA/CCS, United States*
*e-mail*: hkgrave@super.org

https://doi.org/10.4153/S0008439525101331 Published online by Cambridge University Press