# Faktorringe van die Gauss-heelgetalle

Cody Patterson en Kirby C. Smith
Departement Wiskunde, Texas A&M Universiteit, College Station, Texas 77843, VSA

Leon van Wyk
Departement Wiskunde, Universiteit Stellenbosch, Privaatsak X1, Matieland 7602

## Uittreksel

*In teenstelling met die faktorringe van $\mathbb{Z}$ (die ring van heelgetalle) wat goed bekend is, naamlik $\mathbb{Z}, \{0\}$ en $\mathbb{Z}_n$ (die ring van heelgetalle modulo $n$), is dieselfde nie waar vir die homomorfe beelde van $\mathbb{Z}[i]$ (die ring van Gauss-heelgetalle) nie. Meer algemeen, laat $m$ enige nie-nul kwadraatvrye heelgetal (positief of negatief) wees, en beskou die integraalgebied $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$. Watter ringe is homomorfe beelde van $\mathbb{Z}[\sqrt{m}]$? Hierdie vraag bied aan studente 'n oneindige aantal ondersoeke (een vir elke $m$) wat slegs voorgraadse Wiskunde vereis. Die doel van hierdie artikel is om as 'n riglyn tot die bepaling van die homomorfe beelde van $\mathbb{Z}[\sqrt{m}]$ te dien deur die Gauss-heelgetalle $\mathbb{Z}[i]$ as 'n voorbeeld te gebruik. Ons gebruik die feit dat $\mathbb{Z}[i]$ 'n hoofideaalgebied is om te bewys dat as $I = (a + bi)$ 'n nie-nul ideaal van $\mathbb{Z}[i]$ is, dan is $\mathbb{Z}[i]/I \cong \mathbb{Z}_n$ vir 'n positiewe heelgetal $n$ as en slegs as $ggd\{a, b\} = 1$, in welke geval $n = a^2 + b^2$. Ons benadering is oorspronklik in die sin dat dit matrikstegnieke gebruik wat gebaseer is op ry-reduksie van matrikse met heeltallige inskrywings. Deur die heelgetalle $n$ te karakteriseer wat die vorm $n = a^2 + b^2$ het, met $ggd\{a, b\} = 1$, verkry ons die hoofresultaat van die artikel, wat beweer dat as $n \geq 2$, dan is $\mathbb{Z}_n$ 'n homomorfe beeld van $\mathbb{Z}[i]$ as en slegs as $2^{\alpha_0} p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ die priemfaktorisering van $n$ is, met $\alpha_0 \in \{0, 1\}$, $p_i \equiv 1 \pmod 4$ en $\alpha_i \geq 0$ vir elke $i \geq 1$. Al die liggame wat homomorfe beelde van $\mathbb{Z}[i]$ is, word ook bepaal.*

## Abstract

*Factor rings of the Gaussian integers*

*Whereas the homomorphic images of $\mathbb{Z}$ (the ring of integers) are well known, namely $\mathbb{Z}, \{0\}$ and $\mathbb{Z}_n$ (the ring of integers modulo $n$), the same is not true for the homomorphic images of $\mathbb{Z}[i]$ (the ring of Gaussian integers). More generally, let $m$ be any nonzero square free integer (positive or negative), and consider the integral domain $\mathbb{Z}[\sqrt{m}] =$*

$\{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$. *Which rings can be homomorphic images of* $\mathbb{Z}[\sqrt{m}]$*? This question offers students an infinite number (one for each* $m$*) of investigations that require only undergraduate mathematics. It is the goal of this article to offer a guide to the investigation of the possible homomorphic images of* $\mathbb{Z}[\sqrt{m}]$ *using the Gaussian integers* $\mathbb{Z}[i]$ *as an example. We use the fact that* $\mathbb{Z}[i]$ *is a principal ideal domain to prove that if* $I = (a+bi)$ *is a nonzero ideal of* $\mathbb{Z}[i]$*, then* $\mathbb{Z}[i]/I \cong \mathbb{Z}_n$ *for a positive integer* $n$ *if and only if* $gcd\{a, b\} = 1$*, in which case* $n = a^2 + b^2$*. Our approach is novel in that it uses matrix techniques based on the row reduction of matrices with integer entries. By characterizing the integers* $n$ *of the form* $n = a^2 + b^2$*, with* $gcd\{a, b\} = 1$*, we obtain the main result of the paper, which asserts that if* $n \geq 2$*, then* $\mathbb{Z}_n$ *is a homomorphic image of* $\mathbb{Z}[i]$ *if and only if the prime decomposition of* $n$ *is* $2^{\alpha_0} p_1^{\alpha_1} \cdots p_k^{\alpha_k}$*, with* $\alpha_0 \in \{0, 1\}$*,* $p_i \equiv 1 \pmod 4$ *and* $\alpha_i \geq 0$ *for every* $i \geq 1$*. All the fields which are homomorpic images of* $\mathbb{Z}[i]$ *are also determined.*

## INLEIDING

In feitlik elke inleidende abstrakte algebrateksboek word die ring $\mathbb{Z}[i]$ van Gauss-heelgetalle bespreek. Daar word dikwels aangetoon dat $\mathbb{Z}[i]$ 'n Euklidiese gebied is, en die inverteerbare elemente, asook die priemelemente in $\mathbb{Z}[i]$, word bepaal (sien [1]). Aangesien $\mathbb{Z}[i]$ 'n Euklidiese gebied is, is dit 'n hoofideaalgebied, en gevolglik is die ideale $I$ van $\mathbb{Z}[i]$ bekend. Die faktorringe $\mathbb{Z}[i]/I$ word egter nie bespreek nie.

Die homomorfe beelde van $\mathbb{Z}$, die ring van heelgetalle, is goed bekend, naamlik $\mathbb{Z}, \{0\}$ en $\mathbb{Z}_n$, die ring van heelgetalle modulo $n$. Dit is gevolglik voor die hand liggend om die homomorfe beelde van $\mathbb{Z}[i]$ te ondersoek. Meer algemeen, as $m$ enige nie-nul kwadraatvrye heelgetal (positief of negatief) is, kan die integraalgebied $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$ beskou word en gevra word wat die homomorfe beelde van $\mathbb{Z}[\sqrt{m}]$ is. Dit bied aan studente die geleentheid om 'n oneindige aantal (een vir elke $m$) ondersoeke, wat slegs voorgraadse Wiskunde vereis, te onderneem.

Die doel van hierdie artikel is om as 'n riglyn te dien tot die bestudering van die moontlike homomorfe beelde van $\mathbb{Z}[\sqrt{m}]$ deur die Gauss-heelgetalle $\mathbb{Z}[i]$ as voorbeeld te gebruik. Ons fokus op die volgende probleme:

(a) Vir watter positiewe heelgetalle $n$ is die ring $\mathbb{Z}_n$ 'n homomorfe beeld van $\mathbb{Z}[i]$?

(b) Indien $\mathbb{Z}_n$ (vir 'n sekere $n$) 'n homomorfe beeld van $\mathbb{Z}[i]$ is, vind 'n epimorfie (dit

wil sê 'n surjektiewe homomorfie) van $\mathbb{Z}[i]$ na $\mathbb{Z}_n$.

(c) Watter liggame is homomorfe beelde van $\mathbb{Z}[i]$?

Die benadering in hierdie artikel tot die vermelde probleme is oorspronklik in die sin dat dit matrikstegnieke gebruik, naamlik ry-reduksie van matrikse met heeltallige inskrywings.

## RESULTATE

Ons begin met drie bekende hulpstellings waarvan die bewyse elementêr is.

**Hulpstelling 1.** Laat $H$ en $K$ ondergroepe van 'n groep $G$ wees, met $K \subseteq H$. As $[G : K]$ eindig is, dan is $[G : H]$ en $[H : K]$ eindig en $[G : K] = [G : H][H : K]$.

**Hulpstelling 2.** Laat $G$ 'n Abelse groep wees met $G = G_1 \oplus \cdots \oplus G_k$, en laat $H = H_1 \oplus \cdots \oplus H_k$ 'n ondergroep van $G$ wees, met $H_i$ 'n ondergroep van $G_i$ vir elke $i$. Dan is $G/H \cong G_1/H_1 \oplus \cdots \oplus G_k/H_k$.

**Hulpstelling 3.** Laat $R$ 'n eindige ring met $n$ elemente, $n \geq 2$, en met eenheidselement 1 wees. As die additiewe groep $(R, +)$ van $R$ siklies is, dan is $R \cong \mathbb{Z}_n$.

Die volgende voorbeeld illustreer 'n tegniek, wat matrikse gebruik, om die struktuur van 'n faktorring $\mathbb{Z}[i]/I$ van $\mathbb{Z}[i]$ te ontdek.

**Voorbeeld.** Watter ring is isomorf aan $\mathbb{Z}[i]/I$, waar $I := (3 + 5i)$ die hoofideaal van $\mathbb{Z}[i]$ voortgebring deur $3 + 5i$ is? Aangesien $(I, +)$ 'n ondergroep van $(\mathbb{Z}[i], +)$ is, en

$$I = \{(3 + 5i)(a + bi) \mid a, b \in \mathbb{Z}\} = \{a(3 + 5i) + b(-5 + 3i) \mid a, b \in \mathbb{Z}\},$$

volg dat $I$ as 'n additiewe groep deur $3+5i$ en $-5+3i$ voortgebring word. Die groepstruktuur van $\mathbb{Z}[i]$ is $\mathbb{Z}\oplus\mathbb{Z}$, waar ons $a+bi$ met $(a, b)$ identifiseer. Met hierdie identifisering word $(I, +)$ dan voortgebring deur $(3, 5)$ en $(-5, 3)$. As ons "ry-reduksie oor die heelgetalle" op die matriks met $[3 \;\; 5]$ en $[-5 \;\; 3]$ as sy rye toepas, verkry ons

$$\begin{bmatrix} 3 & 5 \\ -5 & 3 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 5 \\ -2 & 8 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 13 \\ -2 & 8 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 13 \\ 0 & 34 \end{bmatrix}.$$

Elke elementêre ry-operasie gee aanleiding tot 'n nuwe matriks waarvan die rye vir $(I,+)$ voortbring. Aangesien $\{(1,13),(0,1)\}$ 'n "basis" vir $(\mathbb{Z}[i],+)$ en

$$\{(1,13),(0,34)\} = \{(1,13),34(0,1)\}$$

'n "basis" vir $(I,+)$ is, volg dit uit Hulpstelling 2 dat die additiewe groep $(\mathbb{Z}[i]/I,+)$ siklies met orde 34 is. Boonop, volgens Hulpstelling 3 is $\mathbb{Z}[i]/I \cong \mathbb{Z}_{34}$. Ons let op dat $34 = 3^2 + 5^2$, wat die norm van die Gauss-heelgetal $3 + 5i$ is.

Die voorafgaande voorbeeld lei tot die volgende algemene resultaat wat die feit gebruik dat elke ideaal van $\mathbb{Z}[i]$ 'n hoofideaal is.

**Stelling 4.** As $I := (a + bi)$ 'n nie-nul ideaal van $\mathbb{Z}[i]$ is, dan is $\mathbb{Z}[i]/I \cong \mathbb{Z}_n$ vir 'n positiewe heelgetal $n$ as en slegs as $\text{ggd}\{a,b\} = 1$, in welke geval $n = a^2 + b^2$.

*Bewys.* Soos reeds gesien in die voorafgaande voorbeeld, word $(I,+)$ voortgebring deur $(a,b)$ en $(-b,a)$. Laat $d := \text{gdd}\{a,b\}$. Dan is $a = da_1$ en $b = db_1$ vir sekere heelgetalle $a_1$ en $b_1$ met $\text{ggd}\{a_1,b_1\} = 1$. Dus is daar heelgetalle $\alpha$ en $\beta$ sodat $a_1\alpha + b_1\beta = 1$, wat impliseer dat $\det(P) = 1$, met

$$P := \begin{bmatrix} \alpha & -\beta \\ b_1 & a_1 \end{bmatrix}.$$

Omdat die rye van

$$A := \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} da_1 & db_1 \\ -db_1 & da_1 \end{bmatrix}$$

vir $(I,+)$ voortbring, en $\det(P) = 1$, bring die rye van

$$PA = \begin{bmatrix} \alpha & -\beta \\ b_1 & a_1 \end{bmatrix} \begin{bmatrix} da_1 & db_1 \\ -db_1 & da_1 \end{bmatrix} = \begin{bmatrix} d & d(b_1\alpha - a_1\beta) \\ 0 & d(a_1^2 + b_1^2) \end{bmatrix}$$

ook vir $(I,+)$ voort. Verder, aangesien $\{(1, b_1\alpha - a_1\beta),(0,1)\}$ 'n basis vir $(\mathbb{Z}[i],+) \cong (\mathbb{Z} \oplus \mathbb{Z},+)$ en $\{(d, d(b_1\alpha - a_1\beta)),(0, d(a_1^2 + b_1^2))\} = \{d(1, b_1\alpha - a_1\beta), d(a_1^2 + b_1^2)(0,1)\}$ 'n basis vir $(I,+)$ is, volg uit Hulpstelling 2 dat

$$(\mathbb{Z}[i]/I,+) \cong (\mathbb{Z}_d \oplus \mathbb{Z}_{d(a_1^2+b_1^2)},+).$$

Gevolglik is die additiewe struktuur van $\mathbb{Z}[i]/I$ siklies as en slegs as $d = 1$, in welke geval $\mathbb{Z}[i]/I \cong \mathbb{Z}_{a_1^2+b_1^2}$. □

**Gevolgtrekking 5.** Laat $(a + bi)$ 'n nie-nul ideaal van $\mathbb{Z}[i]$ wees. Dan is

$$(\mathbb{Z}[i]/(a+bi),+) \cong (\mathbb{Z}_{\text{ggd\{a,b\}}} \oplus \mathbb{Z}_{\frac{a^2+b^2}{\text{ggd\{a,b\}}}},+)$$

en die ring $\mathbb{Z}[i]/(a+bi)$ is eindig met orde $a^2+b^2$.

*Bewys.* In die bewys van Stelling 4 is dit aangetoon dat die groepstruktuur van $\mathbb{Z}[i]/(a+bi)$ isomorf is aan die groep $\mathbb{Z}_d \oplus \mathbb{Z}_{d(a_1^2+b_1^2)}$, dit wil sê die groep $\mathbb{Z}_{\text{ggd}\{a,b\}} \oplus \mathbb{Z}_{\frac{a^2+b^2}{\text{ggd}\{a,b\}}}$. $\square$

Stelling 4 beweer dat $\mathbb{Z}[i]/(a+bi)$ isomorf is aan die ring $Z_n$ as en slegs as $n = a^2 + b^2$ vir heelgetalle $a$ en $b$ met $\text{ggd}\{a,b\} = 1$. In Gevolgtrekking 7 stel ons 'n konkrete (ring)epimorfie van $\mathbb{Z}[i]$ na $\mathbb{Z}_{a^2+b^2}$ met kern $(a+bi)$ ten toon. Ons bewys egter eers die volgende hulpstelling.

**Hulpstelling 6.** Laat $a$ en $b$ heelgetalle wees met $\text{ggd}\{a,b\} = 1$, en laat $\alpha$ en $\beta$ heelgetalle wees sodat $a\alpha + b\beta = 1$. Dan is $(b\alpha - a\beta)^2 \equiv -1 \pmod{a^2+b^2}$.

*Bewys.* Aangesien $a\alpha + b\beta = 1$, is

$$\begin{aligned}(b\alpha - a\beta)^2 + 1 &= b^2\alpha^2 - 2ab\alpha\beta + a^2\beta^2 + (a\alpha + b\beta)^2 \\ &= a^2(\alpha^2+\beta^2) + b^2(\alpha^2+\beta^2) \\ &= (a^2+b^2)(\alpha^2+\beta^2),\end{aligned}$$

wat die bewys voltooi. $\square$

**Gevolgtrekking 7.** Laat $a$ en $b$ heelgetalle wees met $\text{ggd}\{a,b\} = 1$, en laat $\alpha$ en $\beta$ heelgetalle wees sodat $a\alpha + b\beta = 1$. Dan is die funksie $f : \mathbb{Z}[i] \to \mathbb{Z}_{a^2+b^2}$, gedefinieer deur

$$f(x+yi) = x + (b\alpha - a\beta)y \pmod{a^2+b^2},$$

'n ringepimorfie van $\mathbb{Z}[i]$ na $\mathbb{Z}_{a^2+b^2}$ met $\ker(f) = (a+bi)$.

*Bewys.* Dit is maklik om aan te toon dat $f$ 'n groepepimorfie is. Verder volg uit Hulpstelling 6 dat $f$ vermenigvuldiging behou. Ons moet dus nog wys dat $\ker(f) = (a+bi)$. Aangesien

$$\begin{aligned}f(a+bi) &\equiv a + (b\alpha - a\beta)b \pmod{a^2+b^2} \\ &\equiv a + b^2\alpha - ab\beta \pmod{a^2+b^2} \\ &\equiv a + b^2\alpha - a(1-a\alpha) \pmod{a^2+b^2} \\ &\equiv (a^2+b^2)\alpha \pmod{a^2+b^2} \\ &\equiv 0 \pmod{a^2+b^2},\end{aligned}$$

is $(a+bi) \subseteq \ker(f)$. Ons het egter reeds genoem dat $f$ surjektief is, en gevolglik is $\mathbb{Z}[i]/\ker(f) \cong \mathbb{Z}_{a^2+b^2} \cong \mathbb{Z}[i]/(a+bi)$, waar die laaste isomorfie uit Stelling 4 volg. Dus, aangesien $[\mathbb{Z}[i] : (a+bi)] = [\mathbb{Z}[i] : \ker(f)][\ker(f) : (a+bi)]$ volgens Hulpstelling 1, lei ons af dat $[\ker(f) : (a+bi)] = 1$. Gevolglik is $\ker(f) = (a+bi)$. $\square$

Stelling 4 lei tot die volgende vraag: Watter heelgetalle $n$ het die vorm $n = a^2 + b^2$, met $\text{ggd}\{a, b\} = 1$?

**Proposisie 8.** 'n Heelgetal $n \geq 2$ is van die vorm $a^2 + b^2$ vir sekere heelgetalle $a$ en $b$ met $\text{ggd}\{a, b\} = 1$ as en slegs as $2^{\alpha_0} p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ die priemfaktorisering van $n$ is, met $\alpha_0 \in \{0, 1\}$, $p_i \equiv 1 \pmod 4$ en $\alpha_i \geq 0$ vir elke $i \geq 1$.

*Bewys.* Neem aan dat $n = a^2 + b^2$ vir sekere heelgetalle $a$ en $b$ met $\text{ggd}\{a, b\} = 1$. Dan is $a$ of $b$, sê $a$, onewe, en dus is $a^2 \equiv 1 \pmod 4$. Verder weet ons dat $b^2 \equiv 0 \pmod 4$ as $b$ ewe is, en dat $b^2 \equiv 1 \pmod 4$ as $b$ onewe is. In beide gevalle is $a^2 + b^2 \not\equiv 0 \pmod 4$, wat impliseer dat $4 \nmid n$, dit wil sê die hoogste mag van 2 wat in die priemfaktorisering van $n$ voorkom, is $2^1 = 2$.

Veronderstel, by wyse van teenspraak, dat $p \mid n$ vir 'n priemgetal $p$ sodat $p \equiv 3 \pmod 4$. Dan is $a^2 + b^2 \equiv 0 \pmod p$, oftewel $a^2 \equiv -b^2 \pmod p$. Let op dat $p \nmid b$, anders is $p$ ook 'n faktor van $a$, wat die aanname weerspreek dat $\text{ggd}\{a, b\} = 1$. Gevolglik is $b$ inverteerbaar modulo $p$, en dus is daar 'n $c$ sodat $bc \equiv 1 \pmod p$. Derhalwe is $(ac)^2 \equiv -b^2c^2 \pmod p$ $\equiv -1 \pmod p$. Dit is egter uit elementêre getalleteorie bekend dat $-1$ nie 'n kwadraat modulo $p$ is nie indien $p$ 'n priemgetal is sodat $p \equiv 3 \pmod 4$. Hierdie teenspraak toon dat $p \nmid n$ as $p$ 'n priemgetal is sodat $p \equiv 3 \pmod 4$. Die "slegs as" gedeelte van die proposisie is hiermee bewys.

Omgekeerd, veronderstel dat $n$ die gegewe priemfaktorisering het. Ons gebruik 'n resultaat van Fermat, wat in [2] bewys word: elke priemgetal $p$ met $p \equiv 1 \pmod 4$ is van die vorm $p = a^2 + b^2$. Ons bewys boonop dat $\text{ggd}\{a, b\} = 1$. Gestel $d \mid a$ en $d \mid b$. Dan is $d \mid p$, wat impliseer dat $d = 1$ of $d = p$. Dit volg geredelik uit die gelykheid $p = a^2 + b^2$ dat die moontlikheid $d = p$ uitgeskakel word, en dus is $d = 1$. Gevolglik is $\text{ggd}\{a, b\} = 1$. Dit impliseer ook dat nog $a$ nog $b$ deelbaar deur $p$ is, want as een van hulle deelbaar deur $p$ is, dan volg uit die gelykheid $p = a^2 + b^2$ dat die ander een ook deelbaar deur $p$ is, wat die feit weerspreek dat $\text{ggd}\{a, b\} = 1$.

Ons sal nou aantoon dat elke mag van 'n priemgetal $p$, met $p \equiv 1 \pmod 4$, geskryf kan word as die som van twee onderlinge priem heelgetalle. Hiervoor gebruik ons induksie. Gestel dat, vir 'n natuurlike getal $k$, is $p^k = x^2 + y^2$ vir sekere onderlinge priem heelgetalle $x$ en $y$. (Let weer op dat nog $x$ nog $y$ deelbaar deur $p$ is, want as een van hulle deelbaar

deur $p$ is, dan is die ander een ook deelbaar deur $p$.) Ons het nou die volgende:

$$\begin{aligned} p^{k+1} = p \cdot p^k = (a^2+b^2)(x^2+y^2) &= a^2x^2 + a^2y^2 + b^2x^2 + b^2y^2 \\ &= (ax-by)^2 + (ay+bx)^2 \\ &= (ax+by)^2 + (ay-bx)^2. \end{aligned}$$

Ons toon aan dat $ax - by$ en $ay + bx$, of, $ax + by$ en $ay - bx$, onderling priem is. Om dit te doen, let ons eerstens op, soos tevore, dat as

$$d_1 \mid ax - by,\ ay + bx \qquad \text{en} \qquad d_2 \mid ax + by,\ ay - bx,$$

dan is

$$d_1 = 1 \ \text{ of } \ d_1 = p \qquad \text{en} \qquad d_2 = 1 \ \text{ of } \ d_2 = p.$$

As $d_1 = p = d_2$, dan is $p \mid ((ax + by) - (ax - by))$. Verder is $(ax + by) - (ax - by) = 2by$, wat nie 'n veelvoud van $p$ is nie, omdat ons vroeër opgemerk het dat $p \nmid b$ en $p \nmid y$. Dus is $d_1 = 1$ of $d_2 = 1$, en gevolglik is $ax - by$ en $ay + bx$, of, $ax + by$ en $ay - bx$, onderling priem. Hiermee is die induksie-gedeelte van die bewys voltooi.

Gestel nou dat $m$ en $n$ onderlinge priemheelgetalle is wat elk geskryf kan word as die som van die kwadrate van twee onderlinge priemheelgetalle:

$$m = a^2 + b^2 \qquad \text{en} \qquad n = c^2 + d^2.$$

Dan is $mn = (ad - bc)^2 + (ac + bd)^2$. Die volgende vergelykings toon aan dat elk van $mc, md, an$ en $bn$ 'n lineêre kombinasie van $ad - bc$ en $ac + bd$ is:

$$\begin{array}{rcrcrcr} -b(ad-bc) & + & a(ac+bd) & = & a^2c + b^2c & = & mc \\ a(ad-bc) & + & b(ac+bd) & = & a^2d + b^2d & = & md \\ d(ad-bc) & + & c(ac+bd) & = & ac^2 + ad^2 & = & an \\ -c(ad-bc) & + & d(ac+bd) & = & bc^2 + bd^2 & = & bn. \end{array}$$

Aangesien $c$ en $d$ onderling priem is, volg dit dus dat $m$ 'n lineêre kombinasie van $mc$ en $md$ is, en gevolglik is $m$ 'n lineêre kombinasie van $ad - bc$ en $ac + bd$. Op 'n soortgelyke manier is $n$ 'n lineêre kombinasie van $ad-bc$ en $ac+bd$. Laastens, omdat $m$ en $n$ onderling priem is, lei ons af dat 1 'n lineêre kombinasie van $ad - bc$ en $ac + bd$ is. Derhalwe is $ad-bc$ en $ac+bd$ onderling priem, en gevolglik is $mn$ die som van die kwadrate van twee onderlinge priemheelgetalle.

Ons voltooi nou die bewys. Eerstens, $2 = 1^2 + 1^2$, met ggd$\{1, 1\} = 1$. Tweedens, ons het aangetoon dat elke $p_i^{\alpha_i}$ die som van die kwadrate van twee onderlinge priemheelgetalle is as $p_i \equiv 1 \pmod 4$. Laastens, aangesien die priemmagte in die priemfaktorisering van $n$ paarsgewys onderling priem is, sluit die voorafgaande argumente die bewys af. $\square$

Alhoewel Proposisie 8 'n bekende resultaat is, is die bewys nuut in die sin dat dit aansienlik minder ingewikkelde resultate gebruik as wat in bestaande bewyse gevind word.

**Stelling 9.** Vir $n \geq 2$ is $\mathbb{Z}_n$ 'n homomorfe beeld van $\mathbb{Z}[i]$ as en slegs as $2^{\alpha_0} p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ die priemfaktorisering van $n$ is, met $\alpha_0 \in \{0, 1\},\ p_i \equiv 1 \pmod 4$ and $\alpha_i \geq 0$ vir elke $i \geq 1$.

Aangesien ons nou weet watter ringe $\mathbb{Z}_n$ homomorfe beelde van $\mathbb{Z}[i]$ is, is dit natuurlik om te vra watter liggame homomorfe beelde van $\mathbb{Z}[i]$ is. Laat $\mathrm{GF}(q)$ die liggaam met $q = p^n$ elemente aandui, met $p$ 'n priemgetal en $n$ 'n positiewe heelgetal. Dan is $\mathrm{GF}(p) = \mathbb{Z}_p$, en volgens Stelling 9 is $\mathrm{GF}(p)$ 'n homomorfe beeld van $\mathbb{Z}[i]$ as en slegs as $p = 2$ of $p \equiv 1 \pmod 4$.

In die bewys van Stelling 4 het ons gesien dat as $(a + bi)$ 'n nie-nul ideaal van $\mathbb{Z}[i]$ is, dan is die additiewe groep van $\mathbb{Z}[i]/(a + bi)$ isomorf aan $\mathbb{Z}_d \oplus \mathbb{Z}_{d(a_1^2+b_1^2)}$, met $d = \mathrm{ggd}\{a, b\}$ en $a = da_1,\ b = db_1$. Hierdie groep kan die additiewe struktuur van 'n liggaam wees wat nie hierbo beskou is nie, naamlik die liggaam $\mathrm{GF}(p^2)$. Dit sal die geval wees as $d = p$ en $a_1^2 + b_1^2 = 1$, dit wil sê wanneer $a + bi \in \{p, -p, pi, -pi\}$. Aangesien $(p) = (-p) = (pi) = (-pi)$ in $\mathbb{Z}[i]$, hoef ons net $\mathbb{Z}[i]/(p)$ te beskou.

**Stelling 10.** Die liggaam $\mathrm{GF}(q)$ is 'n homomorfe beeld van $\mathbb{Z}[i]$ as en slegs as

(a) $q = p$, met $p = 2$ of $p$ 'n priemgetal sodat $p \equiv 1 \pmod 4$, of

(b) $q = p^2$, met $p$ 'n priemgetal sodat $p \equiv 3 \pmod 4$.

*Bewys.* In die lig van bostaande bespreking hoef ons slegs aan (b) aandag te skenk. Laat $p$ 'n priemgetal wees. Dan is

$$\mathbb{Z}[i]/(p) \cong \{a + b\alpha \mid a, b \in \mathbb{Z}_p \text{ en } \alpha \text{ is 'n simbool met } \alpha^2 = -1 = p - 1\},$$

waar optelling en vermenigvuldiging modulo $p$ is. As $p = 2$, dan is

$$(1 + \alpha)(1 + \alpha) = 1 + 2\alpha + \alpha^2 = 2\alpha = 0,$$

en dus is $\mathbb{Z}[i]/(2)$ nie 'n liggaam nie. Trouens, dit is maklik om te kontroleer dat $\mathbb{Z}[i]/(2)$ isomorf is aan die faktorring $\mathbb{Z}_2[x]/(x^2)$ van die polinoomring $\mathbb{Z}_2[x]$.

Gestel nou dat $p \equiv 1 \pmod 4$. Dan is daar 'n unieke $a$ in $\mathbb{Z}_p$ sodat $2a = 1$, sowel as twee verskillende elemente $b_1, b_2$ in $\mathbb{Z}_p$ sodat $(2b_1)^2 = -1 = (2b_2)^2$. Aangesien $2b_1$ en $2b_2$ beide

wortels van $x^2+1=0$ is, volg dat $b_1+b_2=0$ en $4b_1b_2=1$. Dus is $a+b_1\alpha \neq a+b_2\alpha$ en

$$(a+b_1\alpha)(a+b_2\alpha) = (a^2-b_1b_2)+a(b_1+b_2)\alpha = a^2-b_1b_2.$$

Verder is $4(a^2-b_1b_2) = (2a)^2-4b_1b_2 = 1^2-1 = 0$, wat impliseer dat $a^2-b_1b_2=0$, omdat $p\equiv 1 \pmod 4$. Gevolglik is $(a+b_1\alpha)(a+b_2\alpha)=0$, waaruit volg dat $\mathbb{Z}[i]/(p)$ nie 'n liggaam is nie. Dit is maklik om aan te toon dat $a+b_1\alpha$ en $a+b_2\alpha$ idempotente met som 1 is, en dus, aangesien hulle onderling ortogonaal is, is $\mathbb{Z}[i]/(p) \cong \mathrm{GF}(p)\oplus\mathrm{GF}(p)$.

Laastens, gestel dat $p\equiv 3 \pmod 4$ en dat $(a+b\alpha)(c+e\alpha)=0$ vir sekere $a,b,c$ en $e$. Dan is $(ac-be)+(ae+bc)\alpha=0$, en dus is $ac-be=0=ae+bc$. Laat $d:=\mathrm{ggd}\{a,b\}$, en laat $a=da_1,\ b=db_1$. Aangesien $ac=be$, lei ons af dat

$$0=a(ae+bc)=a^2e+abc=a^2e+b^2e=d^2(a_1^2+b_1^2)e.$$

Derhalwe is $p \mid d^2(a_1^2+b_1^2)e$, en dus is $p\mid d$ of $p\mid (a_1^2+b_1^2)$ of $p\mid e$. As $p\mid d$, dan is $a,b=0$ (in $\mathbb{Z}[i]/(p)$). As $p\mid (a_1^2+b_1^2)$, dan volg uit Proposisie 8 dat $a_1^2+b_1^2=0$, want $\mathrm{ggd}\{a_1,b_1\}=1$ en $p\equiv 3 \pmod 4$. Dit impliseer weer dat $a,b=0$. As $p\mid e$, dan lei ons uit die gelykheid $ac-be=0=ae+bc$ af dat $p\mid ac$ en $p\mid bc$. Gevolglik is $p\mid a,b$ of $p\mid c$, en dus is $a,b=0$ of $c=0$. Derhalwe is $a+b\alpha=0$ of $c+e\alpha=0$. Ons kom tot die slotsom dat $\mathbb{Z}[i]/(p)$ 'n integraalgebied is. Uit Gevolgtrekking 5 sien ons dat $\mathbb{Z}[i]/(p)$ eindig is (met orde $p^2$), en dus is dit 'n liggaam, dit wil sê $\mathbb{Z}[i]/(p)\cong \mathrm{GF}(p^2)$. □

As $\mathrm{ggd}\{a,b\}\neq 1$, dan is dit moeiliker om die struktuur van die faktorring $\mathbb{Z}[i]/(a+bi)$ te bepaal. Ons sluit die artikel af met 'n resultaat in hierdie verband.

**Proposisie 11.** Gestel dat $\mathrm{ggd}\{a,b\}=d$, met $a=da_1$ en $b=db_1$. As $d$ en $a_1^2+b_1^2$ onderling priem is, dan is

$$\mathbb{Z}[i]/(a+bi)\cong \mathbb{Z}[i]/(d)\oplus\mathbb{Z}_{a_1^2+b_1^2}.$$

*Bewys.* Laat $I=(d)$ en $J=(a_1+b_1i)$. Aangesien $a+bi=d(a_1+b_1i)$, is $(a+bi)\subseteq I,J$, en $a_1^2+b_1^2=(a_1+b_1i)(a_1-b_1i)\in J$. Verder is $I+J=(d)+(a_1^2+b_1^2)=\mathbb{Z}[i]$, want $\mathrm{ggd}\{d,a_1^2+b_1^2\}=1$. Definieer $\phi:\mathbb{Z}[i]\to\mathbb{Z}[i]/(d)\oplus\mathbb{Z}[i]/(a_1+b_1i)$ deur $\phi(z)=(z+I,z+J)$. Dit is maklik om te kontroleer dat $\phi$ 'n ringhomomorfie is. Aangesien $\mathrm{ggd}\{d,a_1^2+b_1^2\}=1$, is daar heelgetalle $\alpha$ en $\beta$ sodat $1=d\alpha+(a_1^2+b_1^2)\beta$. Laat $(z_1+I,z_2+J)\in\mathbb{Z}[i]/I\oplus\mathbb{Z}[i]/J$ en laat $w=(a_1^2+b_1^2)\beta z_1+d\alpha z_2$. Dan is $(w+I,w+J)=(z_1+I,z_2+J)$, wat aantoon dat $\phi$ surjektief is.

Ons weet dat $(a+bi) \subseteq \ker(\phi) \subseteq \mathbb{Z}[i]$, en uit Gevolgtrekking 5 sien ons dat $\mathbb{Z}[i]/(a+bi)$ orde $a^2+b^2$ het. Aangesien $\phi$ surjektief is, volg dat $\mathbb{Z}[i]/\ker(\phi) \cong \mathbb{Z}[i]/(d) \oplus \mathbb{Z}[i]/(a_1+b_1i)$, en dus het $\mathbb{Z}[i]/\ker(\phi)$ orde $d^2(a_1^2+b_1^2) = a^2+b^2$. Dit volg dus soos in die laaste gedeelte van die bewys van Gevolgtrekking 7 dat $[\ker(\phi) : (a+bi)] = 1$. Derhalwe is $\ker(\phi) = (a+bi)$. Daarom is

$$\begin{aligned} \mathbb{Z}[i]/(a+bi) &\cong \mathbb{Z}[i]/(d) \oplus \mathbb{Z}[i]/(a_1+b_1i) \\ &\cong \mathbb{Z}[i]/(d) \oplus \mathbb{Z}_{a_1^2+b_1^2}, \end{aligned}$$

waar die laaste isomorfie uit Stelling 4 volg. □

## Summary

In virtually every introductory abstract algebra text the ring $\mathbb{Z}[i]$ of Gaussian integers is introduced. It is frequently shown to be a Euclidean domain, and the units and primes in $\mathbb{Z}[i]$ are discussed (see [1]). Since $\mathbb{Z}[i]$ is an Euclidean domain, it is a principal ideal domain. Hence the ideals $I$ of $\mathbb{Z}[i]$ are known. However, the factor rings $\mathbb{Z}[i]/I$ are not discussed.

The homomorphic images of $\mathbb{Z}$ are well known, namely $\mathbb{Z}$, $\{0\}$ and $\mathbb{Z}_n$, the ring of integers modulo $n$. So it seems natural to investigate the homomorphic images of $\mathbb{Z}[i]$. More generally, let $m \neq 0$ be any square free integer (positive or negative), and consider the integral domain $\mathbb{Z}[\sqrt{m}\,] = \{a+b\sqrt{m} \mid a, b \in \mathbb{Z}\}$. Which rings can be homomorphic images of $\mathbb{Z}[\sqrt{m}\,]$? This offers the student an infinite number (one for each $m$) of investigations that require only undergraduate mathematics.

It is the goal of this article to offer a guide to the investigation of the possible homomorphic images of $\mathbb{Z}[\sqrt{m}\,]$ using the Gaussian integers $\mathbb{Z}[i]$ as an example. Our approach to these problems is novel in that it uses matrix techniques - the row reduction of matrices with integer entries.

The following problems are the main focus of the paper:

(a) For which positive integers $n$ is the ring $\mathbb{Z}_n$ a homomorphic image of $\mathbb{Z}[i]$?

(b) Given that $\mathbb{Z}_n$ is a homomorphic image of $\mathbb{Z}[i]$, exhibit a homomorphism from $\mathbb{Z}[i]$ onto $\mathbb{Z}_n$.

(c) Which fields are homomorphic images of $\mathbb{Z}[i]$?

As far as (a) is concerned, it is shown in Theorem 4 that if $I = (a+bi)$ is a nonzero ideal of $\mathbb{Z}[i]$, then $\mathbb{Z}[i]/I \cong \mathbb{Z}_n$ for some positive integer $n$ if and only if $\gcd\{a,b\} = 1$, in which case $n = a^2 + b^2$. The proof of Theorem 4 also shows that if $(a + bi)$ is a nonzero ideal of $\mathbb{Z}[i]$, then

$$(\mathbb{Z}[i]/(a+bi), +) \cong (\mathbb{Z}_{\gcd\{a,b\}} \oplus \mathbb{Z}_{\frac{a^2+b^2}{\gcd\{a,b\}}}, +)$$

and the ring $\mathbb{Z}[i]/(a+bi)$ is finite with order $a^2 + b^2$.

Even if one knows that $\mathbb{Z}_n$ is a homomorphic image of $\mathbb{Z}[i]$ for some $n$, then, since the proof of Theorem 4 is not constructive, one still does not have a concrete homomorphism from $\mathbb{Z}[i]$ onto $\mathbb{Z}_n$. In Corollary 7 such a homomorphism is exhibited, answering (b). To be precise, let $a$ and $b$ be nonzero integers with $\gcd\{a,b\} = 1$, and let $\alpha$ and $\beta$ be integers such that $1 = a\alpha + b\beta$. Then the map $f : \mathbb{Z}[i] \to \mathbb{Z}_{a^2+b^2}$, defined by

$$f(x+yi) = x + (b\alpha - a\beta)y \pmod{a^2+b^2},$$

is a ring homomorphism from $\mathbb{Z}[i]$ onto $\mathbb{Z}_{a^2+b^2}$ with $\ker(f) = (a+bi)$.

Theorem 4 and Corollary 7 lead to the following question: which integers $n$ have the form $n = a^2 + b^2$, with $\gcd\{a,b\} = 1$? This question is addressed in Proposition 8, in which it is shown that an integer $n \geq 2$ has the form $a^2 + b^2$ for some integers $a$ and $b$, with $\gcd\{a,b\} = 1$, if and only if the prime decomposition of $n$ is $2^{\alpha_0} p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $\alpha_0 \in \{0,1\}$, $p_i \equiv 1 \pmod 4$ and $\alpha_i \geq 0$ for every $i \geq 1$. Although this result is not new, our proof uses much less involved mathematics machinery than the previously known proofs.

The foregoing results culminate in Theorem 9, which states that if $n \geq 2$, then $\mathbb{Z}_n$ is a homomorphic image of $\mathbb{Z}[i]$ if and only if $2^{\alpha_0} p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the prime decomposition of $n$, where $\alpha_0 \in \{0,1\}$, $p_i \equiv 1 \pmod 4$ and $\alpha_i \geq 0$ for every $i \geq 1$.

Problem (c) ties in with Problem (a). Let $\mathrm{GF}(q)$ denote the finite field of $q = p^n$ elements for some prime number $p$ and some positive integer $n$. In Theorem 10 we prove that $\mathrm{GF}(q)$ is a homomorphic image of $\mathbb{Z}[i]$ if and only if

(a) $q = p$, where $p = 2$ or $p$ is a prime number such that $p \equiv 1 \pmod 4$, or

(b) $q = p^2$, where $p$ is a prime number such that $p \equiv 3 \pmod 4$.

The paper is concluded by showing in Proposition 11 that if $\gcd\{a,b\} \neq 1$, then determining the structure of the factor ring $\mathbb{Z}[i]/(a+bi)$ becomes much more involved.

## LITERATUURVERWYSINGS

1. Fraleigh, J.B. (1998). *A First Course in Abstract Algebra, 6th edition* (Addison-Wesley, London).

2. LeVeque, W.J. (1996). *Fundamentals of Number Theory* (Dover Publications, New York).

Wat die derde outeur betref, word hierdie navorsing deur die Nasionale Navorsingstigting van Suid-Afrika met behulp van Toekenning nommer 2053726 ondersteun. Enige menings, bevindings en gevolgtrekkings of aanbevelings is die outeur s'n en reflekteer nie noodwendig die gesigspunte van die Nasionale Navorsingstigting nie.

Hierdie navorsing het 'n aanvang geneem terwyl die derde outeur gedurende 2002-2003 met navorsingsverlof by Texas A&M Universiteit was. Hy spreek sy dank teenoor die lede van die Departement Wiskunde van Texas A&M Universiteit uit vir hul gasvryheid tydens vermelde besoek.