University of Minnesota, School of Mathematics

Math 4281: Introduction to Modern Algebra, Spring 2019: Homework 5

Darij Grinberg

May 15, 2019

1 Exercise 1: Sums of powers of divisors

1.1 Problem

Let n be a positive integer. Let $k \in \mathbb{N}$. Prove that

$$\sum_{d \mid n} d^k = \prod_{p \text{ prime}} \left(p^{0k} + p^{1k} + \cdots + p^{v_p(n) \cdot k} \right).$$

Here, the summation sign "$\sum_{d \mid n}$" means a sum over all **positive** divisors d of n.

1.2 Solution

See the class notes, where this is Exercise 2.18.1 **(b)**. (The numbering may shift; it is one of the exercises in the "Counting divisors" section.)

2 Exercise 2: Another version of Jacobi's two-squares theorem

2.1 Problem

Let n be a positive integer. Prove that

$$\begin{aligned}&\left(\text{the number of pairs } (x,y) \in \mathbb{Z}^2 \text{ such that } n = x^2+y^2\right)\\ &= 4\left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 1 \mod 4\right)\\ &\quad - 4\left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 3 \mod 4\right).\end{aligned}$$

[**Hint:** The formula for the left hand side that we proved in class can be freely used.]

2.2 Solution sketch

Let

$$\begin{aligned}z = &\left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 1 \mod 4\right)\\ &- \left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 3 \mod 4\right).\end{aligned} \tag{1}$$

We shall prove that

$$\left(\text{the number of pairs } (x,y) \in \mathbb{Z}^2 \text{ such that } n = x^2+y^2\right) = 4z. \tag{2}$$

First, we recall some results from the class notes.
Exercise 2.18.2 in the class notes[1] says the following:

Claim 1: **(a)** If there exists a prime p satisfying $p \equiv 3 \bmod 4$ and $v_p(n) \equiv 1 \bmod 2$, then $z = 0$.

(b) If there exists no prime p satisfying $p \equiv 3 \bmod 4$ and $v_p(n) \equiv 1 \bmod 2$, then

$$z = \prod_{\substack{p \text{ prime};\\ p \equiv 1 \bmod 4}} \left(v_p(n)+1\right).$$

On the other hand, a result we proved in class (currently Theorem 4.2.62 in the class notes, but this is likely to shift) states the following:

Claim 2: **(a)** If there is at least one prime $p \equiv 3 \bmod 4$ such that $v_p(n)$ is odd, then there is **no** pair $(x,y) \in \mathbb{Z}^2$ such that $n = x^2+y^2$.

(b) Assume that for each prime $p \equiv 3 \bmod 4$, the number $v_p(n)$ is even. Then,

$$\left(\text{the number of pairs } (x,y) \in \mathbb{Z}^2 \text{ such that } n = x^2+y^2\right) = 4 \cdot \prod_{\substack{p \text{ prime};\\ p \equiv 1 \bmod 4}} \left(v_p(n)+1\right).$$

Now, we are in one of the following two cases:
Case 1: There exists a prime p satisfying $p \equiv 3 \bmod 4$ and $v_p(n) \equiv 1 \bmod 2$.
Case 2: There exists no prime p satisfying $p \equiv 3 \bmod 4$ and $v_p(n) \equiv 1 \bmod 2$.

[1] The numbering may shift; it is one of the exercises in the "Counting divisors" section.

Let us first consider Case 1. In this case, there exists a prime p satisfying $p \equiv 3 \bmod 4$ and $v_p(n) \equiv 1 \bmod 2$. In other words, there is at least one prime $p \equiv 3 \bmod 4$ such that $v_p(n)$ is odd. Thus, Claim 2 **(a)** shows that there is **no** pair $(x, y) \in \mathbb{Z}^2$ such that $n = x^2 + y^2$. Hence,

$$\left(\text{the number of pairs } (x, y) \in \mathbb{Z}^2 \text{ such that } n = x^2 + y^2\right) = 0. \tag{3}$$

On the other hand, Claim 1 **(a)** yields $z = 0$, so that $4z = 0$. Comparing this with (3), we obtain

$$\left(\text{the number of pairs } (x, y) \in \mathbb{Z}^2 \text{ such that } n = x^2 + y^2\right) = 4z.$$

Hence, (2) is proven in Case 1.

Let us next consider Case 2. In this case, there exists no prime p satisfying $p \equiv 3 \bmod 4$ and $v_p(n) \equiv 1 \bmod 2$. In other words, there exists no prime $p \equiv 3 \bmod 4$ for which $v_p(n)$ is odd. In other words, for each prime $p \equiv 3 \bmod 4$, the number $v_p(n)$ is even. Hence, Claim 2 **(b)** shows that

$$\left(\text{the number of pairs } (x, y) \in \mathbb{Z}^2 \text{ such that } n = x^2 + y^2\right) = 4 \cdot \prod_{\substack{p \text{ prime;} \\ p \equiv 1 \bmod 4}} \left(v_p(n) + 1\right).$$

On the other hand,

$$4 \underbrace{z}_{= \prod\limits_{\substack{p \text{ prime;} \\ p \equiv 1 \bmod 4}} (v_p(n)+1) \text{ (by Claim 1 (b))}} = 4 \cdot \prod_{\substack{p \text{ prime;} \\ p \equiv 1 \bmod 4}} \left(v_p(n) + 1\right).$$

Comparing these two equalities, we obtain

$$\left(\text{the number of pairs } (x, y) \in \mathbb{Z}^2 \text{ such that } n = x^2 + y^2\right) = 4z.$$

Hence, (2) is proven in Case 2.

We have now proven (2) in each of the two Cases 1 and 2. Thus, (2) always holds.

Now, (2) becomes

$$\begin{aligned}
&\left(\text{the number of pairs } (x, y) \in \mathbb{Z}^2 \text{ such that } n = x^2 + y^2\right) \\
&= 4z \\
&= 4 \big(\text{(the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 1 \mod 4\big) \\
&\qquad - \text{(the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 3 \mod 4)\big) \\
&\qquad \text{(by (1))} \\
&= 4 \,\text{(the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 1 \mod 4) \\
&\qquad - 4 \,\text{(the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 3 \mod 4).
\end{aligned}$$

This solves the exercise.

2.3 Remark

For some completely different solutions of the above exercise (using formal power series instead of Gaussian integers), see Hirschhorn's [Hirsch85, Theorem 1] and [Hirsch17, Chapter 2]. See also [UspHea39, Chapter XIII] for related results.

3 Exercise 3: Characterizing Gaussian primes

3.1 Problem

Let π be a Gaussian prime.

Prove the following:

(a) If π is unit-equivalent to an integer, then π is unit-equivalent to a prime[2] of Type 3.

(Recall that a prime p is said to be *of Type 3* if it is congruent to 3 modulo 4.)

Assume, from now on, that π is **not** unit-equivalent to any integer. Let $(p_1, p_2, \ldots, p_k)$ be a prime factorization of the positive integer $\mathrm{N}(\pi)$. (Thus, $p_1, p_2, \ldots, p_k$ are primes such that $\mathrm{N}(\pi) = p_1 p_2 \cdots p_k$.)

(b) Prove that $\pi \mid p_i$ for some $i \in \{1, 2, \ldots, k\}$.

Fix an $i \in \{1, 2, \ldots, k\}$ such that $\pi \mid p_i$.

(c) Prove that $p_i = \pi\overline{\pi}$.

(d) Prove that p_i is a prime of Type 1 or of Type 2.

(Recall that a prime p is said to be *of Type 1* if it is congruent to 1 modulo 4, and is said to be *of Type 2* if it equals 2.)

3.2 Remark

This exercise yields that the Gaussian primes are the primes of Type 3 and the Gaussian prime divisors of the primes of Types 1 and 2 (up to unit-equivalence). Conversely, any of the latter are indeed Gaussian primes (as we proved in class). This completes the characterization of Gaussian primes. See also [ConradG, Theorem 9.9] for a different proof of this fact.

3.3 Solution sketch

First, we notice that π is neither zero nor a unit (since π is a Gaussian prime); thus, $\mathrm{N}(\pi)$ is neither 0 nor 1. Hence, $\mathrm{N}(\pi) > 1$ (since $\mathrm{N}(\pi) \in \mathbb{N}$). In particular, $\mathrm{N}(\pi)$ is a positive integer and $\mathrm{N}(\pi) \neq 1$.

(a) Assume that π is unit-equivalent to an integer. In other words, $\pi \sim g$ for some $g \in \mathbb{Z}$. Consider this g.

We have $\pi \sim g \sim -g$. Thus, π is unit-equivalent to both g and $-g$. Hence, we can WLOG assume that $g \geq 0$ (since otherwise, we can simply replace g by $-g$). Assume this.

The integer g is a Gaussian integer; it is unit-equivalent to a Gaussian prime (namely, to π), and thus itself is a Gaussian prime[3]. Thus, each Gaussian divisor of g is either a unit or unit-equivalent to g (by the definition of a Gaussian prime).

We know from class (Proposition 4.2.15 in the class notes) that unit-equivalent Gaussian integers have equal norms. Hence, from $\pi \sim g$, we obtain $\mathrm{N}(\pi) = \mathrm{N}(g) = g^2$ (since $g \in \mathbb{Z} \subseteq \mathbb{R}$). Thus, $g^2 = \mathrm{N}(\pi) > 1$, so that $g > 1$ (since $g \geq 0$).

[2]The unqualified word "prime" always means a prime in the original sense, i.e., an integer $p > 1$ whose only positive divisors are 1 and p.

[3]because any Gaussian integer that is unit-equivalent to a Gaussian prime must itself be a Gaussian prime

Hence, if g was not a prime, then g would have a positive divisor other than 1 and g. This positive divisor would then be a Gaussian divisor of g, but it would not be a unit (since it is a positive integer distinct from 1); therefore, it would be unit-equivalent to g (since each Gaussian divisor of g is either a unit or unit-equivalent to g). But this would contradict the fact that its norm is smaller than the norm of g (indeed, it is a positive integer smaller than g, so that its norm is smaller than the norm of g), whereas unit-equivalent Gaussian integers must have equal norms. Hence, we would obtain a contradiction. This shows that g must be a prime.

But we know (from what is currently Theorem 4.2.42 **(d)** in the class notes) that if p is a prime of Type 2 or Type 1, then p is not a Gaussian prime. Hence, g cannot be a prime of Type 2 or Type 1 (because g is a Gaussian prime). Thus, g must be a prime of Type 3 (since g is a prime). Thus, π is unit-equivalent to a prime of Type 3 (namely, to g). This solves part **(a)** of the exercise.

(b) We have $\mathrm{N}(\pi) = p_1 p_2 \cdots p_k$ (since $(p_1, p_2, \ldots, p_k)$ is a prime factorization of $\mathrm{N}(\pi)$). But $\mathrm{N}(\pi) = \pi\overline{\pi}$. Hence, $\pi \mid \pi\overline{\pi} = \mathrm{N}(\pi) = p_1 p_2 \cdots p_k$.

Proposition 2.13.7 in the class notes says that if a prime p divides a product $a_1 a_2 \cdots a_k$ of k integers $a_1, a_2, \ldots, a_k$, then p must divide (at least) one of these integers $a_1, a_2, \ldots, a_k$. The same argument can be used to prove the analogous fact about Gaussian primes: Namely, if a Gaussian prime ψ divides a product $\alpha_1 \alpha_2 \cdots \alpha_k$ of k Gaussian integers $\alpha_1, \alpha_2, \ldots, \alpha_k$, then ψ must divide (at least) one of these Gaussian integers $\alpha_1, \alpha_2, \ldots, \alpha_k$. Applying this to $\psi = \pi$ and $\alpha_i = p_i$, we conclude that π must divide (at least) one of these Gaussian integers $p_1, p_2, \ldots, p_k$ (since π divides their product $p_1 p_2 \cdots p_k$). In other words, $\pi \mid p_i$ for some $i \in \{1, 2, \ldots, k\}$. This solves part **(b)** of the exercise.

(c) We have $\pi \mid p_i$. Thus, $p_i = \pi\alpha$ for some Gaussian integer α. Consider this α. From $p_i = \pi\alpha$, we obtain $\mathrm{N}(p_i) = \mathrm{N}(\pi\alpha) = \mathrm{N}(\pi)\,\mathrm{N}(\alpha)$, so that $\mathrm{N}(\pi)\,\mathrm{N}(\alpha) = \mathrm{N}(p_i) = p_i^2$ (since $p_i \in \mathbb{Z} \subseteq \mathbb{R}$). Thus, $p_i^2 = \mathrm{N}(\pi)\,\mathrm{N}(\alpha)$, so that $\mathrm{N}(\pi) \mid p_i^2$. Hence, $\mathrm{N}(\pi)$ is a positive divisor of p_i^2 (since $\mathrm{N}(\pi)$ is a positive integer).

We assumed that π is **not** unit-equivalent to any integer. Thus, in particular, π is not unit-equivalent to p_i. In other words, we don't have $\pi \sim p_i$. In other words, we don't have $p_i \sim \pi$.

If we had $\mathrm{N}(\alpha) = 1$, then α would be a unit, and thus we would have $p_i \sim \pi$ (since $p_i = \pi\alpha$); but this would contradict the fact that we don't have $p_i \sim \pi$. Hence, we don't have $\mathrm{N}(\alpha) = 1$. Thus, $\mathrm{N}(\alpha) \neq 1$.

If we had $\mathrm{N}(\pi) = p_i^2$, then we would have $p_i^2 = \underbrace{\mathrm{N}(\pi)}_{=p_i^2}\mathrm{N}(\alpha) = p_i^2\,\mathrm{N}(\alpha)$ and thus $\mathrm{N}(\alpha) = 1$, which would contradict $\mathrm{N}(\alpha) \neq 1$. Hence, we have $\mathrm{N}(\pi) \neq p_i^2$.

But the positive divisors of p_i^2 are 1, p_i and p_i^2 (since p_i is a prime). Hence, $\mathrm{N}(\pi)$ must be either 1 or p_i or p_i^2 (since $\mathrm{N}(\pi)$ is a positive divisor of p_i^2). Since $\mathrm{N}(\pi)$ cannot be 1 or p_i^2 (because $\mathrm{N}(\pi) \neq 1$ and $\mathrm{N}(\pi) \neq p_i^2$), we thus have $\mathrm{N}(\pi) = p_i$. Hence, $p_i = \mathrm{N}(\pi) = \pi\overline{\pi}$. This solves part **(c)** of the exercise.

(d) Assume the contrary. Thus, p_i is a prime of Type 3 (since p_i is a prime). Hence, $p_i \equiv 3 \bmod 4$.

However, write the Gaussian integer π as $\pi = (a, b)$ with $a, b \in \mathbb{Z}$. Part **(c)** of this exercise yields $p_i = \pi\overline{\pi} = \mathrm{N}(\pi) = a^2 + b^2$ (since $\pi = (a, b)$). Thus, $a^2 + b^2 = p_i \equiv 3 \bmod 4$.

But recall that no two integers x and y satisfy $x^2 + y^2 \equiv 3 \bmod 4$ (by Exercise 2.7.2 **(c)** in the class notes). This contradicts the fact that the two integers a and b do satisfy

$a^2 + b^2 \equiv 3 \bmod 4$. This contradiction shows that our assumption was wrong. This solves part **(d)** of the exercise.

---

4 Exercise 4: Gaussian integers modulo a Gaussian integer

4.1 Problem

For any Gaussian integer τ, we let $\underset{\tau}{\equiv}$ be the binary relation on $\mathbb{Z}[i]$ defined by

$$\left(\alpha \underset{\tau}{\equiv} \beta\right) \iff (\alpha \equiv \beta \mod \tau).$$

It is straightforward to see (just as in the case of integers) that this relation $\underset{\tau}{\equiv}$ is an equivalence relation. (You don't need to prove this.) We shall refer to the equivalence classes of this relation $\underset{\tau}{\equiv}$ as the *Gaussian residue classes modulo* τ; let $\mathbb{Z}[i]/\tau$ be the set of all these classes.

Let n be a nonzero integer.

Prove that the equivalence classes of the relation $\underset{n}{\equiv}$ (on $\mathbb{Z}[i]$) are the n^2 classes $[a+bi]_{\underset{n}{\equiv}}$ for $a, b \in \{0, 1, \ldots, |n|-1\}$, and that these n^2 classes are all distinct.

4.2 Remark

This exercise yields $|\mathbb{Z}[i]/n| = n^2 = \mathrm{N}(n)$ for any nonzero integer n. This is [ConradG, Lemma 7.15]. (Conrad proves this "by example"; you can follow the argument but you should write it up in full generality.)

More generally, $|\mathbb{Z}[i]/\tau| = \mathrm{N}(\tau)$ for any nonzero Gaussian integer τ. This is proven in [ConradG, Theorem 7.14] (using the above exercise as a stepping stone).

4.3 Solution sketch

We shall use the following fact (which is Exercise 4.2.11 **(b)** in the class notes):

> *Claim 1:* Let n be a positive integer. Then, the equivalence classes of the relation $\underset{n}{\equiv}$ (on $\mathbb{Z}[i]$) are the n^2 classes $[a+bi]_{\underset{n}{\equiv}}$ for $a, b \in \{0, 1, \ldots, n-1\}$, and these n^2 classes are all distinct.

Claim 1 is precisely the statement of our exercise in the case when n is positive (because in this case, we have $|n| = n$). Thus, the exercise is solved in this case. Hence, for the rest of this solution, we WLOG assume that n is not positive. Hence, n is negative (since n is nonzero). Thus, $-n$ is positive, and $|n| = -n$.

We notice that the relations $\underset{n}{\equiv}$ (on $\mathbb{Z}[i]$) and $\underset{-n}{\equiv}$ (on $\mathbb{Z}[i]$) are identical[4]. But Claim 1 (applied to $-n$ instead of n) shows that the equivalence classes of the relation $\underset{-n}{\equiv}$ (on

[4] *Proof.* In order to see this, we merely need to check that for any two Gaussian integers α and β, the two statements $\left(\alpha \underset{n}{\equiv} \beta\right)$ and $\left(\alpha \underset{-n}{\equiv} \beta\right)$ are equivalent. Let us do this now: Let α and β be two Gaussian

$\mathbb{Z}[i]$) are the $(-n)^2$ classes $[a+bi]_{\equiv_{-n}}$ for $a, b \in \{0, 1, \ldots, (-n)-1\}$, and these $(-n)^2$ classes are all distinct. In view of $(-n)^2 = n^2$ and $\underbrace{(-n)}_{=|n|} - 1 = |n| - 1$, this rewrites as follows: The equivalence classes of the relation $\underset{-n}{\equiv}$ (on $\mathbb{Z}[i]$) are the n^2 classes $[a+bi]_{\equiv_{-n}}$ for $a, b \in \{0, 1, \ldots, |n|-1\}$, and these n^2 classes are all distinct. Since the relations $\underset{n}{\equiv}$ (on $\mathbb{Z}[i]$) and $\underset{-n}{\equiv}$ (on $\mathbb{Z}[i]$) are identical, we can further rewrite this as follows: The equivalence classes of the relation $\underset{n}{\equiv}$ (on $\mathbb{Z}[i]$) are the n^2 classes $[a+bi]_{\equiv_n}$ for $a, b \in \{0, 1, \ldots, |n|-1\}$, and these n^2 classes are all distinct. This solves the exercise.

---

5 Exercise 5: A Fibonacci divisibility

5.1 Problem

Let $\phi = \dfrac{1+\sqrt{5}}{2}$ and $\psi = \dfrac{1-\sqrt{5}}{2}$ be the two (real) roots of the polynomial $x^2 - x - 1$. (The number ϕ is known as the *golden ratio.*) It is easy to see that $\phi + \psi = 1$ and $\phi \cdot \psi = -1$.

Let $\mathbb{Z}[\phi]$ be the set of all reals of the form $a + b\phi$ with $a, b \in \mathbb{Z}$.

(a) Prove that any $\alpha, \beta \in \mathbb{Z}[\phi]$ satisfy $\alpha + \beta \in \mathbb{Z}[\phi]$ and $\alpha - \beta \in \mathbb{Z}[\phi]$ and $\alpha\beta \in \mathbb{Z}[\phi]$.

(In the terminology of abstract algebra, this is saying that $\mathbb{Z}[\phi]$ is a subring of $\mathbb{R}$.)

(b) Prove that every element of $\mathbb{Z}[\phi]$ can be written as $a + b\phi$ for a **unique** pair (a, b) of integers. (In other words, if four integers a, b, c, d satisfy $a + b\phi = c + d\phi$, then $a = c$ and $b = d$.)

Given two elements α and β of $\mathbb{Z}[\phi]$, we say that $\alpha \mid \beta$ *in* $\mathbb{Z}[\phi]$ if and only if there exists some $\gamma \in \mathbb{Z}[\phi]$ such that $\beta = \alpha\gamma$. Thus, we have defined divisibility in $\mathbb{Z}[\phi]$. Basic properties of divisibility of integers (such as Proposition 2.2.4) still apply to divisibility in $\mathbb{Z}[\phi]$ (with the same proofs).

---

integers. We have the logical implication $(n \mid \alpha - \beta) \implies (-n \mid \alpha - \beta)$ (because if we have $n \mid \alpha - \beta$, then $-n \mid n \mid \alpha - \beta$) and the logical implication $(-n \mid \alpha - \beta) \implies (n \mid \alpha - \beta)$ (because if we have $-n \mid \alpha - \beta$, then $n \mid -n \mid \alpha - \beta$). Combining these two implications, we obtain the equivalence $(n \mid \alpha - \beta) \iff (-n \mid \alpha - \beta)$.

Now, we have the following chain of equivalences:

$$
\begin{aligned}
&\left(\alpha \underset{n}{\equiv} \beta\right) \\
&\iff (\alpha \equiv \beta \bmod n) && \left(\text{by the definition of the relation } \underset{n}{\equiv}\right) \\
&\iff (n \mid \alpha - \beta) && \text{(by the definition of congruence)} \\
&\iff (-n \mid \alpha - \beta) \\
&\iff (\alpha \equiv \beta \bmod -n) && \text{(by the definition of congruence)} \\
&\iff \left(\alpha \underset{-n}{\equiv} \beta\right) && \left(\text{by the definition of the relation } \underset{-n}{\equiv}\right).
\end{aligned}
$$

In other words, the two statements $\left(\alpha \underset{n}{\equiv} \beta\right)$ and $\left(\alpha \underset{-n}{\equiv} \beta\right)$ are equivalent. Qed.

(c) If a and b are two elements of $\mathbb{Z}$ such that $a \mid b$ in $\mathbb{Z}[\phi]$, then prove that $a \mid b$ in $\mathbb{Z}$.

Let $(f_0, f_1, f_2, \ldots)$ be the sequence of nonnegative integers defined recursively by

$$f_0 = 0, \qquad f_1 = 1, \qquad \text{and} \qquad f_n = f_{n-1} + f_{n-2} \text{ for all } n \geq 2.$$

This is the so-called *Fibonacci sequence* (and continues with $f_2 = 1$, $f_3 = 2$, $f_4 = 3$, $f_5 = 5$ etc.).

It is well-known (*Binet's formula*) that

$$f_n = \frac{\phi^n - \psi^n}{\sqrt{5}} \qquad \text{for all } n \geq 0. \tag{4}$$

(You don't need to prove this; there is a completely straightforward proof by induction on n.)

(d) Prove that $f_d \mid f_{dn}$ for any nonnegative integers d and n.

[**Hint:** Lemma 2.10.11 **(a)** holds not just for integers.]

5.2 Remark

This exercise (specifically its part **(d)**) is an example of how a property of integers (here, $f_d \mid f_{dn}$) can often be proved by working in a larger domain (in our case, $\mathbb{Z}[\phi]$). Another example is our study of sums of two perfect squares using Gaussian integers (done in class). There are various others. While part **(d)** of this exercise has fairly simple solutions using integer arithmetic alone, some other properties of Fibonacci numbers are best understood by means of working in $\mathbb{Z}[\phi]$. For example, if $p \neq 5$ is a prime, then one of the two Fibonacci numbers f_{p-1} and f_{p+1} is divisible by p, while the other is $\equiv 1 \mod p$.

5.3 Solution sketch

(a) This solution will be very similar to the solution of Exercise 4 **(a)** on homework set #4. The main difference is that $\sqrt{2}$ gets replaced by ϕ, which behaves slightly differently when being squared.

It is easy to see (from the definition of ϕ) that $\phi^2 = \phi + 1$.

Let $\alpha, \beta \in \mathbb{Z}[\phi]$. We must prove that $\alpha + \beta \in \mathbb{Z}[\phi]$ and $\alpha - \beta \in \mathbb{Z}[\phi]$ and $\alpha\beta \in \mathbb{Z}[\phi]$.

We have $\alpha \in \mathbb{Z}[\phi]$. In other words, α is a real of the form $a + b\phi$ with $a, b \in \mathbb{Z}$ (by the definition of $\mathbb{Z}[\phi]$). In other words, there exist two integers $x_1, x_2 \in \mathbb{Z}$ such that $\alpha = x_1 + x_2\phi$. Similarly, there exist two integers $y_1, y_2 \in \mathbb{Z}$ such that $\beta = y_1 + y_2\phi$. Consider these four integers x_1, x_2, y_1, y_2.

We have

$$\underbrace{\alpha}_{=x_1+x_2\phi} + \underbrace{\beta}_{=y_1+y_2\phi} = (x_1 + x_2\phi) + (y_1 + y_2\phi) = (x_1 + y_1) + (x_2 + y_2)\,\phi.$$

Hence, $\alpha + \beta$ is a real of the form $a + b\phi$ with $a, b \in \mathbb{Z}$ (namely, with $a = x_1 + y_1$ and $b = x_2 + y_2$). In other words, $\alpha + \beta \in \mathbb{Z}[\phi]$ (by the definition of $\mathbb{Z}[\phi]$).

We have

$$\underbrace{\alpha}_{=x_1+x_2\phi} - \underbrace{\beta}_{=y_1+y_2\phi} = (x_1 + x_2\phi) - (y_1 + y_2\phi) = (x_1 - y_1) + (x_2 - y_2)\,\phi.$$

Hence, $\alpha - \beta$ is a real of the form $a + b\phi$ with $a, b \in \mathbb{Z}$ (namely, with $a = x_1 - y_1$ and $b = x_2 - y_2$). In other words, $\alpha - \beta \in \mathbb{Z}[\phi]$ (by the definition of $\mathbb{Z}[\phi]$).

We have

$$\begin{aligned}
\underbrace{\alpha}_{=x_1+x_2\phi}\underbrace{\beta}_{=y_1+y_2\phi} &= (x_1 + x_2\phi)(y_1 + y_2\phi) = x_1y_1 + x_1y_2\phi + x_2\phi y_1 + x_2\phi y_2\phi \\
&= x_1y_1 + x_1y_2\phi + x_2\underbrace{\phi y_1}_{=y_1\phi} + x_2\underbrace{\phi y_2}_{=y_2\phi}\phi \\
&= x_1y_1 + x_1y_2\phi + x_2y_1\phi + x_2y_2\underbrace{\phi\phi}_{=\phi^2=\phi+1} \\
&= x_1y_1 + x_1y_2\phi + x_2y_1\phi + x_2y_2(\phi + 1) \\
&= (x_1y_1 + x_2y_2) + (x_1y_2 + x_2y_1 + x_2y_2)\phi. \qquad (5)
\end{aligned}$$

Hence, $\alpha\beta$ is a real of the form $a + b\phi$ with $a, b \in \mathbb{Z}$ (namely, with $a = x_1y_1 + x_2y_2$ and $b = x_1y_2 + x_2y_1 + x_2y_2$). In other words, $\alpha\beta \in \mathbb{Z}[\phi]$ (by the definition of $\mathbb{Z}[\phi]$).

We have now shown that $\alpha + \beta \in \mathbb{Z}[\phi]$ and $\alpha - \beta \in \mathbb{Z}[\phi]$ and $\alpha\beta \in \mathbb{Z}[\phi]$. This solves part **(a)** of the exercise.

(b) This solution will be very similar to the solution of Exercise 4 **(b)** on homework set #4. The main difference is that $\sqrt{2}$ gets replaced by ϕ, which has a slightly different reason to be irrational.

Let α be an element of $\mathbb{Z}[\phi]$. We must prove that α can be written as $a + b\phi$ for a **unique** pair (a, b) of integers.

Clearly, α can be written as $a + b\phi$ for **at least one** pair (a, b) of integers (because this is what it means for α to belong to $\mathbb{Z}[\phi]$). Thus, it remains to prove that α can be written as $a + b\phi$ for **at most one** pair (a, b) of integers. In other words, we must prove that if (a_1, b_1) and (a_2, b_2) are two pairs (a, b) of integers such that $\alpha = a + b\phi$, then $(a_1, b_1) = (a_2, b_2)$.

Let us prove this. Let (a_1, b_1) and (a_2, b_2) be two pairs (a, b) of integers such that $\alpha = a + b\phi$. We must show that $(a_1, b_1) = (a_2, b_2)$.

Assume the contrary. Thus, $(a_1, b_1) \neq (a_2, b_2)$.

It is easy to check that 5 is not a perfect square[5]. Exercise 2.10.15 **(a)** in the class notes shows that if a positive integer u is not a perfect square, then $\sqrt{u}$ is irrational. Applying this to $u = 5$, we conclude that $\sqrt{5}$ is irrational (since 5 is not a perfect square).

From $\phi = \dfrac{1 + \sqrt{5}}{2}$, we obtain $2\phi = 1 + \sqrt{5}$, so that $\sqrt{5} = 2\phi - 1$. Hence, if the number ϕ was rational, then $\sqrt{5}$ would be rational as well, which would contradict the fact that $\sqrt{5}$ is irrational. Hence, the number ϕ cannot be rational. In other words, ϕ is irrational.

But (a_1, b_1) is a pair (a, b) of integers such that $\alpha = a + b\phi$. In other words, (a_1, b_1) is a pair of integers and satisfies $\alpha = a_1 + b_1\phi$. Similarly, (a_2, b_2) is a pair of integers and satisfies $\alpha = a_2 + b_2\phi$. Hence, $a_2 + b_2\phi = \alpha = a_1 + b_1\phi$, so that

$$a_2 - a_1 = b_1\phi - b_2\phi = (b_1 - b_2)\phi. \qquad (6)$$

[5] *Proof.* Assume the contrary. Thus, 5 is a perfect square. In other words, $5 = u^2$ for some $u \in \mathbb{Z}$. Consider this u. If we had $|u| \geq 3$, then we would have $|u|^2 \geq 3^2 = 9 > 5$, which would contradict $|u|^2 = u^2 = 5$. Hence, we cannot have $|u| \geq 3$. Thus, $|u| < 3$, so that $u \in \{-2, -1, 0, 1, 2\}$ (since u is an integer). Hence, $u^2 \in \left\{(-2)^2, (-1)^2, 0^2, 1^2, 2^2\right\} = \{4, 1, 0, 1, 4\}$. This contradicts $u^2 = 5$. This contradiction shows that our assumption was false, qed.

If we had $b_1 = b_2$, then this would yield $a_2 - a_1 = \underbrace{(b_1 - b_2)}_{\substack{=0 \\ (\text{since } b_1 = b_2)}} \phi = 0$, which would lead to $a_1 = a_2$ and therefore $\left(\underbrace{a_1}_{=a_2}, \underbrace{b_1}_{=b_2} \right) = (a_2, b_2)$; but this would contradict $(a_1, b_1) \neq (a_2, b_2)$. Hence, we cannot have $b_1 = b_2$. Thus, we have $b_1 \neq b_2$. In other words, $b_1 - b_2 \neq 0$. Hence, we can divide both sides of the equality (6) by $b_1 - b_2$. We thus obtain $\dfrac{a_2 - a_1}{b_1 - b_2} = \phi$. Hence, the number $\dfrac{a_2 - a_1}{b_1 - b_2}$ is irrational (since ϕ is irrational). But this contradicts the fact that $\dfrac{a_2 - a_1}{b_1 - b_2}$ is rational (which is clear, since a_1, a_2, b_1, b_2 are integers). This contradiction shows that our assumption was wrong. Hence, $(a_1, b_1) = (a_2, b_2)$ is proven. This completes our solution of part **(b)** of the exercise.

(c) Let a and b be two elements of $\mathbb{Z}[\phi]$ such that $a \mid b$ in $\mathbb{Z}[\phi]$. We must prove that $a \mid b$ in $\mathbb{Z}$.

We WLOG assume that $b \neq 0$, since otherwise this follows trivially from $b = 0 = a \cdot 0$.

We have $a \mid b$ in $\mathbb{Z}[\phi]$. In other words, there exists some $\gamma \in \mathbb{Z}[\phi]$ such that $b = a\gamma$ (by the definition of divisibility in $\mathbb{Z}[\phi]$). Consider this γ. From $a\gamma = b \neq 0$, we obtain $a \neq 0$.

We have $\gamma \in \mathbb{Z}[\phi]$. In other words, γ is a real of the form $x_1 + x_2\phi$ with $x_1, x_2 \in \mathbb{Z}$ (by the definition of $\mathbb{Z}[\phi]$). Consider these x_1 and x_2. We have

$$b = a \underbrace{\gamma}_{=x_1 + x_2\phi} = a(x_1 + x_2\phi) = ax_1 + ax_2\phi.$$

If we had $ax_2 \neq 0$, then we could solve this equality for ϕ and obtain $\phi = \dfrac{b - ax_1}{ax_2}$; this would yield that ϕ is rational (since b, a, x_1, x_2 are integers), and this would contradict the fact that ϕ is irrational (as we have shown in our above solution to part **(b)** of this exercise). Hence, we cannot have $ax_2 \neq 0$. Thus, we have $ax_2 = 0$. Since $a \neq 0$, this leads to $x_2 = 0$. Hence, $\gamma = x_1 + \underbrace{x_2}_{=0}\phi = x_1 \in \mathbb{Z}$. Thus, from $b = a\gamma$, we obtain $a \mid b$ in $\mathbb{Z}$. This solves part **(c)** of the exercise.

(d) We have $\phi + \psi = 1$, thus $\psi = 1 - \phi = 1 + (-1)\phi$. Hence, $\psi \in \mathbb{Z}[\phi]$.

In part **(a)** of this exercise, we have shown that the product of two elements of $\mathbb{Z}[\phi]$ belongs to $\mathbb{Z}[\phi]$ again. Thus, by induction, we can easily see that a product of any (finite) number of elements of $\mathbb{Z}[\phi]$ belongs to $\mathbb{Z}[\phi]$ again. Hence, in particular, if $\alpha \in \mathbb{Z}[\phi]$ and $k \in \mathbb{N}$, then $\alpha^k \in \mathbb{Z}[\phi]$. Thus, the powers ϕ^d, ϕ^{dn}, ψ^d and ψ^{dn} belong to $\mathbb{Z}[\phi]$ (since ϕ and ψ belong to $\mathbb{Z}[\phi]$).

We recall the following fact (Lemma 2.10.11 **(a)** in the class notes):

> *Claim 1:* Let $d \in \mathbb{N}$. Let x and y be integers. Then, $x - y \mid x^d - y^d$.

This fact has an analogue for elements of $\mathbb{Z}[\phi]$ instead of integers:

> *Claim 2:* Let $d \in \mathbb{N}$. Let x and y be elements of $\mathbb{Z}[\phi]$. Then, $x - y \mid x^d - y^d$ in $\mathbb{Z}[\phi]$.

[*Proof of Claim 2:* Both proofs we gave for Claim 1 in the class notes can be modified in an obvious way to yield proofs of Claim 2.]

Now, let d and n be nonnegative integers. We must prove that $f_d \mid f_{dn}$.

Applying (4) to d instead of n, we find

$$f_d = \frac{\phi^d - \psi^d}{\sqrt{5}}.$$

Multiplying both sides of this equality with $\sqrt{5}$, we obtain

$$\sqrt{5} \cdot f_d = \phi^d - \psi^d. \tag{7}$$

The same argument (applied to dn instead of n) yields

$$\sqrt{5} \cdot f_{dn} = \phi^{dn} - \psi^{dn}. \tag{8}$$

Now, ϕ^d and ψ^d are elements of $\mathbb{Z}[\phi]$ (as we know). Hence, Claim 2 (applied to n, ϕ^d and ψ^d instead of d, x and y) yields $\phi^d - \psi^d \mid \left(\phi^d\right)^n - \left(\psi^d\right)^n$ in $\mathbb{Z}[\phi]$. In view of

$$\phi^d - \psi^d = \sqrt{5} \cdot f_d \qquad \text{(by (7))}$$

and

$$\left(\phi^d\right)^n - \left(\psi^d\right)^n = \phi^{dn} - \psi^{dn} = \sqrt{5} \cdot f_{dn} \qquad \text{(by (8))},$$

this rewrites as $\sqrt{5} \cdot f_d \mid \sqrt{5} \cdot f_{dn}$ in $\mathbb{Z}[\phi]$. In other words, there exists a $\delta \in \mathbb{Z}[\phi]$ such that $\sqrt{5} \cdot f_{dn} = \sqrt{5} \cdot f_d \cdot \delta$ (by the definition of divisibility in $\mathbb{Z}[\phi]$). Consider this δ. Cancelling $\sqrt{5}$ from the equation $\sqrt{5} \cdot f_{dn} = \sqrt{5} \cdot f_d \cdot \delta$, we obtain $f_{dn} = f_d \cdot \delta$. Since $\delta \in \mathbb{Z}[\phi]$, this shows that $f_d \mid f_{dn}$ in $\mathbb{Z}[\phi]$ (by the definition of divisibility in $\mathbb{Z}[\phi]$). Thus, part **(c)** of this exercise (applied to $a = f_d$ and $b = f_{dn}$) shows that $f_d \mid f_{dn}$ in $\mathbb{Z}$ (since f_d and f_{dn} are elements of $\mathbb{Z}$). This solves part **(d)** of the exercise.

---

6 Exercise 6: Non-unique factorization in $\mathbb{Z}\left[\sqrt{-3}\right]$

6.1 Problem

We let $\sqrt{-3}$ denote the complex number $\sqrt{3}i$.

Let $\mathbb{Z}\left[\sqrt{-3}\right]$ be the set of all complex numbers of the form $a + b\sqrt{-3}$ with $a, b \in \mathbb{Z}$. These complex numbers are called the 3-*Gaussian integers*.

It is easy to see that the set $\mathbb{Z}\left[\sqrt{-3}\right]$ is closed under addition, subtraction and multiplication (i.e., that any $\alpha, \beta \in \mathbb{Z}\left[\sqrt{-3}\right]$ satisfy $\alpha + \beta \in \mathbb{Z}\left[\sqrt{-3}\right]$ and $\alpha - \beta \in \mathbb{Z}\left[\sqrt{-3}\right]$ and $\alpha\beta \in \mathbb{Z}\left[\sqrt{-3}\right]$). (In the terminology of abstract algebra, this is saying that $\mathbb{Z}\left[\sqrt{-3}\right]$ is a subring of $\mathbb{C}$.)

It is also easy to see that each element of $\mathbb{Z}\left[\sqrt{-3}\right]$ can be written as $a + b\sqrt{-3}$ for a **unique** pair (a, b) of integers.

(a) Prove that each 3-Gaussian integer α satisfies $\mathrm{N}(\alpha) \in \mathbb{N}$ and $\mathrm{N}(\alpha) \not\equiv 2 \mod 3$.

(Recall that $\mathrm{N}(\alpha)$ is defined for every complex number α, and thus for every 3-Gaussian integer α, since 3-Gaussian integers are complex numbers.)

Given two elements α and β of $\mathbb{Z}\left[\sqrt{-3}\right]$, we say that $\alpha \mid \beta$ *in* $\mathbb{Z}\left[\sqrt{-3}\right]$ if and only if there exists some $\gamma \in \mathbb{Z}\left[\sqrt{-3}\right]$ such that $\beta = \alpha\gamma$. Thus, we have defined divisibility in $\mathbb{Z}\left[\sqrt{-3}\right]$. Basic properties of divisibility of integers (such as Proposition 2.2.4) still apply to divisibility in $\mathbb{Z}\left[\sqrt{-3}\right]$ (with the same proofs).

If $\alpha \in \mathbb{Z}\left[\sqrt{-3}\right]$, then a 3-*Gaussian divisor of* α shall mean a $\beta \in \mathbb{Z}\left[\sqrt{-3}\right]$ such that $\beta \mid \alpha$ in $\mathbb{Z}\left[\sqrt{-3}\right]$.

We define the notions of "inverse", "unit" and "unit-equivalent" for 3-Gaussian integers as we did for Gaussian integers.

A nonzero 3-Gaussian integer π that is not a unit is called a 3-*Gaussian prime* if each 3-Gaussian divisor of π is either a unit or unit-equivalent to π.

(b) List all the 3-Gaussian integers having norms < 4.

(c) List all units in $\mathbb{Z}\left[\sqrt{-3}\right]$.

(d) Prove that 2, $1+\sqrt{-3}$ and $1-\sqrt{-3}$ are 3-Gaussian primes.

(e) Prove that $2 \cdot 2 = \left(1+\sqrt{-3}\right) \cdot \left(1-\sqrt{-3}\right)$.

(f) Define two 3-Gaussian integers α and β by $\alpha = 2$ and $\beta = 1+\sqrt{-3}$. Prove that there exist no 3-Gaussian integers γ and ρ such that $\alpha = \gamma\beta + \rho$ and $\mathrm{N}(\rho) < \mathrm{N}(\beta)$.

[**Hint:** Your list in part **(b)** should contain 5 entries. Your list in part **(c)** should contain 2 entries: Unlike the ring $\mathbb{Z}[i]$ with its 4 units, the ring $\mathbb{Z}\left[\sqrt{-3}\right]$ has only 2 units.

For **(d)**, discuss the norm of any possible 3-Gaussian divisor.]

6.2 Remark

Parts **(d)** and **(e)** of this exercise show that unique factorization into primes is not automatically preserved when we extend a number system. Neither is division with remainder, as part **(f)** illustrates (though we already have seen the geometric reason for this in class). (Neither is the existence of a well-behaved greatest common divisor.)

6.3 Solution sketch

(a) Let α be a 3-Gaussian integer. Thus, $\alpha = a+b\sqrt{-3}$ for some $a, b \in \mathbb{Z}$ (by the definition of a 3-Gaussian integer). Consider these a and b. We have $\alpha = a+b\underbrace{\sqrt{-3}}_{=\sqrt{3}i} = a+b\sqrt{3}i = \left(a, b\sqrt{3}\right)$ (regarded as a complex number). Hence, the definition of the norm of a complex number yields $\mathrm{N}(\alpha) = a^2 + \underbrace{\left(b\sqrt{3}\right)^2}_{=3b^2} = a^2+3b^2 \in \mathbb{N}$ (since a^2 and b^2 are squares of integers and therefore belong to $\mathbb{N}$). It remains to prove that $\mathrm{N}(\alpha) \not\equiv 2 \mod 3$.

Corollary 2.6.9 **(a)** in the class notes (applied to $u = a$ and $n = 3$) shows that $a\%3 \in \{0, 1, \ldots, 3-1\}$ and $a\%3 \equiv a \mod 3$. Thus, $a\%3 \in \{0, 1, \ldots, 3-1\} = \{0, 1, 2\}$, so that $a\%3$ is either 0 or 1 or 2. Thus, we are in one of the following three cases:

Case 1: We have $a\%3 = 0$.

Case 2: We have $a\%3 = 1$.

Case 3: We have $a\%3 = 2$.

Let us first consider Case 3. In this case, we have $a\%3 = 2$. But we can take the congruence $a\%3 \equiv a \mod 3$ to the 2-nd power; thus we obtain $(a\%3)^2 \equiv a^2 \mod 3$. In view of $a\%3 = 2$, this rewrites as $2^2 \equiv a^2 \mod 3$. Hence, $a^2 \equiv 2^2 = 4 \mod 3$. Now, $\mathrm{N}(\alpha) = a^2 + \underbrace{3b^2}_{\equiv 0 \mod 3} \equiv a^2 \equiv 4 \not\equiv 2 \mod 3$. Thus, our claim $\mathrm{N}(\alpha) \not\equiv 2 \mod 3$ is proven in Case 3.

Similarly, this claim can be proven in Case 1 and in Case 2. Thus, the claim is proven in all cases. This completes the solution of part **(a)** of this exercise.

(b) We claim that:

- The only 3-Gaussian integer having norm 0 is 0.
- The only 3-Gaussian integers having norm 1 are 1 and -1.
- There are no 3-Gaussian integers having norm 2.
- The only 3-Gaussian integers having norm 3 are $\sqrt{-3}$ and $-\sqrt{-3}$.

More generally: If N is a nonnegative integer, then we can find all 3-Gaussian integers α having norm N by a straightforward exhaustive check of all possible cases. Indeed, if α is a 3-Gaussian integer having norm N, then we can write α in the form $\alpha = a + b\sqrt{-3}$ for some $a, b \in \mathbb{Z}$ (since α is a 3-Gaussian integer), and then we have $N = \mathrm{N}(\alpha) = a^2 + 3b^2$ (as we have seen in the solution to part **(a)** of this exercise); but this entails that both integers a and b lie between $-\sqrt{N}$ and $\sqrt{N}$ (since $N = a^2 + 3\underbrace{b^2}_{\geq 0} \geq a^2$ and $N = \underbrace{a^2}_{\geq 0} + 3b^2 \geq 3b^2 = 2\underbrace{b^2}_{\geq 0} + b^2 \geq b^2$), and this leaves only finitely many possibilities for a and b, which can all be directly checked. Thus our above four claims can be proven.

(c) We claim that the units in $\mathbb{Z}\left[\sqrt{-3}\right]$ are 1 and -1.

[*Proof.* It is clear that 1 and -1 are units in $\mathbb{Z}\left[\sqrt{-3}\right]$ (since each of the numbers 1 and -1 is its own inverse, and thus has an inverse in $\mathbb{Z}\left[\sqrt{-3}\right]$, which means that it is a unit in $\mathbb{Z}\left[\sqrt{-3}\right]$). Thus, it remains to show that there are no other units. In other words, it remains to show that each unit in $\mathbb{Z}\left[\sqrt{-3}\right]$ is either 1 or -1. In other words, it remains to show that if α is a unit in $\mathbb{Z}\left[\sqrt{-3}\right]$, then $\alpha = 1$ or $\alpha = -1$.

So let α be a unit in $\mathbb{Z}\left[\sqrt{-3}\right]$. We must show that $\alpha = 1$ or $\alpha = -1$.

We know that α is a unit in $\mathbb{Z}\left[\sqrt{-3}\right]$. In other words, α has an inverse in $\mathbb{Z}\left[\sqrt{-3}\right]$. Consider this inverse $\alpha^{-1} \in \mathbb{Z}\left[\sqrt{-3}\right]$. Thus, α^{-1} is a 3-Gaussian integer.

Part **(a)** of this exercise yields $\mathrm{N}(\alpha) \in \mathbb{N}$. The same argument (applied to α^{-1} instead of α) yields $\mathrm{N}(\alpha^{-1}) \in \mathbb{N}$ (since α^{-1} is a 3-Gaussian integer).

But $\alpha\alpha^{-1} = 1$ and thus $\mathrm{N}(\alpha\alpha^{-1}) = \mathrm{N}(1) = 1^2 = 1$, so that $1 = \mathrm{N}(\alpha\alpha^{-1}) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\alpha^{-1})$. This leads to $\mathrm{N}(\alpha) \mid 1$ (since $\mathrm{N}(\alpha^{-1}) \in \mathbb{N}$). Therefore, $\mathrm{N}(\alpha) = 1$ (since $\mathrm{N}(\alpha) \in \mathbb{N}$). In other words, α is a 3-Gaussian integer having norm 1. Since we already know (from our solution to part **(b)** of this exercise) that the only 3-Gaussian integers having norm 1 are 1 and -1, we thus conclude that α is either 1 or -1 [6]. In other words,

[6] Here is a simpler way of proving this: We know that α is a 3-Gaussian integer. Thus, $\alpha = a + b\sqrt{-3}$ for some $a, b \in \mathbb{Z}$ (by the definition of a 3-Gaussian integer). Consider these a and b. We have $\mathrm{N}(\alpha) = a^2 + 3b^2$ (as we have already shown when solving part **(a)** of this exercise), so that $a^2 + 3b^2 = \mathrm{N}(\alpha) = 1$. If the integer

$\alpha = 1$ or $\alpha = -1$. This completes our proof.]

(d) Let us first prove that 2 is a 3-Gaussian prime:

Claim 1: The 3-Gaussian integer 2 is a 3-Gaussian prime.

[*Proof of Claim 1:* Indeed, 2 is clearly a nonzero 3-Gaussian integer that is not a unit[7]. Thus, in order to prove Claim 1, we only need to check that each 3-Gaussian divisor of 2 is either a unit or unit-equivalent to 2.

So let us prove this. Let δ be a 3-Gaussian divisor of 2. We must prove that δ is either a unit or unit-equivalent to 2.

We have seen (in the solution to part **(c)** of this exercise) that the only 3-Gaussian integers having norm 1 are 1 and -1. Thus, all 3-Gaussian integers having norm 1 are units (since 1 and -1 are units).

We know that δ is a 3-Gaussian divisor of 2. In other words, there exists a 3-Gaussian integer γ such that $2 = \delta\gamma$. Consider this γ. From $2 = \delta\gamma$, we obtain $\mathrm{N}(2) = \mathrm{N}(\delta\gamma) = \mathrm{N}(\delta) \cdot \mathrm{N}(\gamma)$, so that $\mathrm{N}(\delta) \cdot \mathrm{N}(\gamma) = \mathrm{N}(2) = 2^2 = 4$.

Part **(a)** of this exercise (applied to $\alpha = \delta$) yields $\mathrm{N}(\delta) \in \mathbb{N}$ and $\mathrm{N}(\delta) \not\equiv 2 \mod 3$. The same argument (applied to γ instead of δ) yields $\mathrm{N}(\gamma) \in \mathbb{N}$ and $\mathrm{N}(\gamma) \not\equiv 2 \mod 3$. Now, the equality $\mathrm{N}(\delta) \cdot \mathrm{N}(\gamma) = 4$ leads to $\mathrm{N}(\delta) \mid 4$ (since $\mathrm{N}(\gamma) \in \mathbb{N}$). Thus, $\mathrm{N}(\delta)$ must be 1, 2 or 4 (since the only divisors of 4 in $\mathbb{N}$ are 1, 2 and 4). Since $\mathrm{N}(\delta) \neq 2$ (because $\mathrm{N}(\delta) \not\equiv 2 \mod 3$), the second of these three possibilities is ruled out; thus, $\mathrm{N}(\delta)$ must be 1 or 4. So we must be in one of the following two cases:

Case 1: We have $\mathrm{N}(\delta) = 1$.

Case 2: We have $\mathrm{N}(\delta) = 4$.

Let us first consider Case 1. In this case, we have $\mathrm{N}(\delta) = 1$. In other words, δ has norm 1. Hence, δ is a unit (since all 3-Gaussian integers having norm 1 are units). Thus, our claim (that δ is either a unit or unit-equivalent to 2) is proven in Case 1.

Let us now consider Case 2. In this case, we have $\mathrm{N}(\delta) = 4$. Comparing $\mathrm{N}(\delta) \cdot \mathrm{N}(\gamma) = 4$ with $\underbrace{\mathrm{N}(\delta)}_{=4} \cdot \mathrm{N}(\gamma) = 4 \cdot \mathrm{N}(\gamma)$, we obtain $4 \cdot \mathrm{N}(\gamma) = 4$, so that $\mathrm{N}(\gamma) = 1$. Thus, γ has norm 1, and therefore γ is a unit (since all 3-Gaussian integers having norm 1 are units). Hence, 2 is unit-equivalent to δ (since $2 = \delta\gamma = \gamma\delta$). In other words, δ is unit-equivalent to 2 (since unit-equivalence is an equivalence relation). Thus, our claim (that δ is either a unit or unit-equivalent to 2) is proven in Case 2.

We have now proven (in both Cases 1 and 2) that δ is either a unit or unit-equivalent to 2. As we know, this completes the proof of Claim 1.]

Thus, we have proven that 2 is a 3-Gaussian prime. The same argument can be used to show that $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ are 3-Gaussian primes (since both $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ have norm 4). Thus, part **(d)** of the exercise is solved.

---

b was nonzero, then its square b^2 would be ≥ 1 (since the square of a nonzero integer is always ≥ 1), and thus we would have $\underbrace{a^2}_{\geq 0} + 3\underbrace{b^2}_{\geq 1} \geq 0 + 3 \cdot 1 = 3 > 1$, which would contradict $a^2 + 3b^2 = 1$. Hence, b cannot be nonzero. In other words, $b = 0$. Hence $a^2 + 3b^2 = a^2 + 3 \cdot 0^2 = a^2$, so that $a^2 = a^2 + 3b^2 = 1$. Thus, a is either 1 or -1. But $\alpha = a + \underbrace{b}_{=0}\sqrt{-3} = a$. Thus, α is either 1 or -1 (since a is either 1 or -1).

[7] Indeed, in part **(c)** of this exercise, we have seen what the units are; 2 is clearly none of them.

(e) This is a straightforward computation.

(f) Assume the contrary. Thus, there exist 3-Gaussian integers γ and ρ such that $\alpha = \gamma\beta + \rho$ and $\mathrm{N}(\rho) < \mathrm{N}(\beta)$. Consider these γ and ρ. Solving the equation $\alpha = \gamma\beta + \rho$ for γ, we obtain $\gamma = \dfrac{\alpha - \rho}{\beta}$ (since $\beta \neq 0$).

A straightforward computation reveals that $\mathrm{N}(\beta) = 4$. Hence, $\mathrm{N}(\rho) < \mathrm{N}(\beta) = 4$. Thus, ρ is a 3-Gaussian integer having norm < 4. But in part **(b)** of this exercise, we have found all such 3-Gaussian integers; namely, they are 0, 1, -1, $\sqrt{-3}$ and $-\sqrt{-3}$. Thus, ρ must be one of the numbers 0, 1, -1, $\sqrt{-3}$ and $-\sqrt{-3}$. This gives five possible cases to check. In each of these five cases, we can compute γ from $\gamma = \dfrac{\alpha - \rho}{\beta}$. We thus obtain the following table of values of γ:

ρ	0	1	-1	$\sqrt{-3}$	$-\sqrt{-3}$
γ	$\frac{1}{2} - \frac{1}{2}\sqrt{-3}$	$\frac{1}{4} - \frac{1}{4}\sqrt{-3}$	$\frac{3}{4} - \frac{3}{4}\sqrt{-3}$	$\frac{-1}{4} - \frac{3}{4}\sqrt{-3}$	$\frac{5}{4} - \frac{1}{4}\sqrt{-3}$

.

(We have used the standard strategy of rationalizing denominators in order to compute these values of γ.) This table makes it clear that (in each of the five cases) γ can be written in the form $\gamma = a + b\sqrt{-3}$ with some numbers $a, b \in \mathbb{Q}$ that are not both integers. But we also know that γ can be written in the form $\gamma = a + b\sqrt{-3}$ with some $a, b \in \mathbb{Z}$ (because $\gamma \in \mathbb{Z}\left[\sqrt{-3}\right]$). Thus, there are (at least) **two** different ways to write γ in the form $\gamma = a + b\sqrt{-3}$ with some numbers $a, b \in \mathbb{Q}$ [8]. But this is impossible, since each element z of $\mathbb{C}$ can be **uniquely** written as $z = a + b\sqrt{-3}$ with $a, b \in \mathbb{R}$ (namely, $a = \operatorname{Re} z$ and $b = \operatorname{Im} z/\sqrt{3}$). This contradiction shows that our assumption was false. Hence, part **(f)** of the exercise is solved.

References

[ConradG] Keith Conrad, *The Gaussian integers*.
`http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/Zinotes.pdf`

[Hirsch17] Michael D. Hirschhorn, *The power of q: a personal journey*, Springer 2017.

[Hirsch85] Michael D. Hirschhorn, *A simple proof of Jacobi's two-square theorem*, Amer. Math. Monthly 92, pp. 579–580 (1985).

[UspHea39] J. V. Uspensky, M. A. Heaslet, *Elementary Number Theory*, McGraw-Hill 1939.

[8] Indeed, the first way uses two numbers a, b that are not both integers, while the second way uses two numbers $a, b \in \mathbb{Z}$, that is, two numbers a, b that are both integers. Thus, the two ways are indeed different.