1 Exercise 1: Sums of powers of divisors

1.1 Problem

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

$$\sum_{d|n} d^k = \prod_{p \text{ prime}} \left( p^{\lfloor \log p \rfloor k} + p^{\lfloor \log p \rfloor} + \cdots + p^{v_p(n)\cdot k} \right).$$

Here, the summation sign "\(\sum\)" 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

\[
(\text{the number of pairs } (x, y) \in \mathbb{Z}^2 \text{ such that } n = x^2 + y^2) \\
= 4 (\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 1 \mod 4) \\
- 4 (\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 3 \mod 4).
\]

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

2.2 Solution sketch

Let

\[
z = (\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 1 \mod 4) \\
- (\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 3 \mod 4). \tag{1}
\]

We shall prove that

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

First, we recall some results from the class notes.

Exercise 2.18.2 in the class notes says the following:

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

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

\[
z = \prod_{p \text{ prime}; \ p \equiv 1 \mod 4} (v_p(n) + 1).
\]

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 \( p \equiv 3 \mod 4 \) 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 \( p \equiv 3 \mod 4 \), the number \( v_p(n) \) is even. Then,

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

Now, we are in one of the following two cases:

Case 1: There exists a prime \( p \) satisfying \( p \equiv 3 \mod 4 \) and \( v_p(n) \equiv 1 \mod 2 \).

Case 2: There exists no prime \( p \) satisfying \( p \equiv 3 \mod 4 \) and \( v_p(n) \equiv 1 \mod 2 \).

\(^1\)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 $p \equiv 3 \mod 4$ and $v_p(n) \equiv 1 \mod 2$. In other words, there is at least one prime $p \equiv 3 \mod 4$ 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,

\[
\text{(the number of pairs } (x, y) \in \mathbb{Z}^2 \text{ such that } n = x^2 + y^2) = 0.
\]

(3)

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

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

Hence, (2) is proven in Case 1.

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

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

On the other hand,

\[
4 \cdot \prod_{\text{p prime;} \ p \equiv 1 \mod 4} (v_p(n) + 1) = 4 \cdot \prod_{\text{p prime;} \ p \equiv 1 \mod 4} (v_p(n) + 1).
\]

Comparing these two equalities, we obtain

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

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

\[
\text{(the number of pairs } (x, y) \in \mathbb{Z}^2 \text{ such that } n = x^2 + y^2)
\]

\[
= 4z
\]

\[
= 4 \left( \text{(the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 1 \mod 4) - \text{(the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 3 \mod 4) \right)
\]

(by (1))

\[
= 4 \left( \text{(the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 1 \mod 4) - 4 \left( \text{(the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 3 \mod 4) \right) \right).
\]

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 $\pi$ be a Gaussian prime. Prove the following:

(a) If $\pi$ is unit-equivalent to an integer, then $\pi$ is unit-equivalent to a prime 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 $\pi$ is not unit-equivalent to any integer. Let $(p_1, p_2, \ldots, p_k)$ be a prime factorization of the positive integer $N(\pi)$. (Thus, $p_1, p_2, \ldots, p_k$ are primes such that $N(\pi) = p_1 p_2 \cdots p_k$.)

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

(a) Assume that $\pi$ 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, $\pi$ 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 $\pi$), and thus itself is a Gaussian prime. 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 $N(\pi) = N(g) = g^2$ (since $g \in \mathbb{Z} \subseteq \mathbb{R}$). Thus, $g^2 = N(\pi) > 1$, so that $g > 1$ (since $g \geq 0$).

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

3because 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, \( \pi \) is unit-equivalent to a prime of Type 3 (namely, to \( g \)). This solves part (a) of the exercise.

(b) We have \( N(\pi) = p_1p_2 \cdots p_k \) (since \( p_1, p_2, \ldots, p_k \) is a prime factorization of \( N(\pi) \)). But \( N(\pi) = \pi \bar{\pi} \). Hence, \( \pi \mid \pi \bar{\pi} = N(\pi) = p_1p_2 \cdots p_k \).

Proposition 2.13.7 in the class notes says that if a prime \( \alpha \) divides a product \( a_1a_2 \cdots a_k \) of \( k \) integers \( a_1, a_2, \ldots, a_k \), then \( \alpha \) 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 \( \psi \) divides a product \( \alpha_1\alpha_2 \cdots \alpha_k \) of Gaussian integers \( \alpha_1, \alpha_2, \ldots, \alpha_k \), then \( \psi \) 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 \( \pi \) must divide (at least) one of these Gaussian integers \( p_1, p_2, \ldots, p_k \) (since \( \pi \) divides their product \( p_1p_2 \cdots p_k \)). 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 \( \alpha \). Consider this \( \alpha \). From \( p_i = \pi \alpha \), we obtain \( N(p_i) = N(\pi \alpha) = N(\pi)N(\alpha) \), so that \( N(\pi)N(\alpha) = N(p_i) = p_i^2 \) (since \( p_i \in \mathbb{Z} \subseteq \mathbb{R} \)). Thus, \( p_i^2 = N(\pi)N(\alpha) \), so that \( N(\pi) \mid p_i^2 \). Hence, \( N(\pi) \) is a positive divisor of \( p_i^2 \) (since \( N(\pi) \) is a positive integer).

We assumed that \( \pi \) is not unit-equivalent to any integer. Thus, in particular, \( \pi \) 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 \( N(\alpha) = 1 \), then \( \alpha \) 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 \( N(\alpha) = 1 \). Thus, \( N(\alpha) \neq 1 \).

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

But the positive divisors of \( p_i^2 \) are 1, \( p_i \) and \( p_i^2 \) (since \( p_i \) is a prime). Hence, \( N(\pi) \) must be either 1 or \( p_i \) or \( p_i^2 \) (since \( N(\pi) \) is a positive divisor of \( p_i^2 \)). Since \( N(\pi) \) cannot be 1 or \( p_i^2 \) (because \( N(\pi) \neq 1 \) and \( N(\pi) \neq p_i^2 \)), we thus have \( N(\pi) = p_i \). Hence, \( p_i = N(\pi) = \pi \bar{\pi} \).

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, \( p_i \equiv 3 \mod 4 \).

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

But recall that no two integers \( x \) and \( y \) satisfy \( x^2 + y^2 \equiv 3 \mod 4 \) (by Exercise 2.7.2 (c) in the class notes). This contradicts the fact that the two integers \( a \) and \( b \) do satisfy...
\[a^2 + b^2 \equiv 3 \text{ mod } 4.\] 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 \(\tau\), we let \(\equiv\) be the binary relation on \(\mathbb{Z}[i]\) defined by

\[(\alpha \equiv \beta) \iff (\alpha \equiv \beta \mod \tau).\]

It is straightforward to see (just as in the case of integers) that this relation \(\equiv\) is an equivalence relation. (You don’t need to prove this.) We shall refer to the equivalence classes of this relation \(\equiv\) as the Gaussian residue classes modulo \(\tau\); 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 \(\equiv\) (on \(\mathbb{Z}[i]\)) are the \(n^2\) classes \([a + bi]_{\equiv}^n\) for \(a, b \in \{0, 1, \ldots, |n| - 1\}\), and that these \(n^2\) classes are all distinct.

4.2 Remark

This exercise yields \(|\mathbb{Z}[i] / n| = n^2 = N(n)\) 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, \(|\mathbb{Z}[i] / \tau| = N(\tau)\) for any nonzero Gaussian integer \(\tau\). 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 4.2.8 (b) in the class notes):

Claim 1: Let \(n\) be a positive integer. Then, the equivalence classes of the relation \(\equiv\) (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.

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 positive, and \(|n| = -n\).

We notice that the relations \(\equiv\) (on \(\mathbb{Z}[i]\)) and \(\equiv\) (on \(\mathbb{Z}[i]\)) are identical. But Claim 1 (applied to \(-n\) instead of \(n\)) shows that the equivalence classes of the relation \(\equiv\) (on \(\mathbb{Z}[i]\)) are the \((-n)^2\) classes \([-a + bi]_{\equiv}^{-n}\) for \(-a, -b \in \{0, 1, \ldots, |\tau| - 1\}\), and these \((-n)^2\) classes are all distinct.

\[a^2 + b^2 \equiv 3 \text{ mod } 4.\] This contradiction shows that our assumption was wrong. This solves part (d) of the exercise.

---

Proof. In order to see this, we merely need to check that for any two Gaussian integers \(\alpha\) and \(\beta\), the two statements \((\alpha \equiv \beta)\) and \((\alpha \equiv \beta)\) are equivalent. Let us do this now: Let \(\alpha\) and \(\beta\) be two Gaussian integers.

\[\alpha \equiv \beta \iff (\alpha \equiv \beta \mod \tau).\]

It is straightforward to see (just as in the case of integers) that this relation \(\equiv\) is an equivalence relation. (You don’t need to prove this.) We shall refer to the equivalence classes of this relation \(\equiv\) as the Gaussian residue classes modulo \(\tau\); 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 \(\equiv\) (on \(\mathbb{Z}[i]\)) are the \(n^2\) classes \([a + bi]_{\equiv}^n\) for \(a, b \in \{0, 1, \ldots, |n| - 1\}\), and that these \(n^2\) classes are all distinct.

4.2 Remark

This exercise yields \(|\mathbb{Z}[i] / n| = n^2 = N(n)\) 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, \(|\mathbb{Z}[i] / \tau| = N(\tau)\) for any nonzero Gaussian integer \(\tau\). 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 4.2.8 (b) in the class notes):

Claim 1: Let \(n\) be a positive integer. Then, the equivalence classes of the relation \(\equiv\) (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.

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 positive, and \(|n| = -n\).

We notice that the relations \(\equiv\) (on \(\mathbb{Z}[i]\)) and \(\equiv\) (on \(\mathbb{Z}[i]\)) are identical. But Claim 1 (applied to \(-n\) instead of \(n\)) shows that the equivalence classes of the relation \(\equiv\) (on \(\mathbb{Z}[i]\)) are the \((-n)^2\) classes \([-a + bi]_{\equiv}^{-n}\) for \(-a, -b \in \{0, 1, \ldots, |\tau| - 1\}\), and these \((-n)^2\) classes are all distinct.

Proof. In order to see this, we merely need to check that for any two Gaussian integers \(\alpha\) and \(\beta\), the two statements \((\alpha \equiv \beta)\) and \((\alpha \equiv \beta)\) are equivalent. Let us do this now: Let \(\alpha\) and \(\beta\) be two Gaussian integers.

\[\alpha \equiv \beta \iff (\alpha \equiv \beta \mod \tau).\]
$\mathbb{Z}[i]$ are the $(-n)^2$ classes $[a + bi]_n^\equiv$ for $a, b \in \{0, 1, \dots, (-n)−1\}$, and these $(-n)^2$ classes are all distinct. In view of $(-n)^2 = n^2$ and $(-n)−1 = |n|−1$, this rewrites as follows:

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

---

5 Exercise 5: A Fibonacci divisibility

5.1 Problem

Let $\phi = \frac{1 + \sqrt{5}}{2}$ and $\psi = \frac{1 - \sqrt{5}}{2}$ be the two (real roots of the polynomial $x^2 − x − 1$. (The number $\phi$ 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 $\alpha$ and $\beta$ of $\mathbb{Z}[\phi]$, we say that $\alpha | \beta$ 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 $(n | \alpha − \beta) \implies (−n | \alpha − \beta)$ (because if we have $n | \alpha − \beta$, then $−n | n | \alpha − \beta$) and the logical implication $(−n | \alpha − \beta) \implies (n | \alpha − \beta)$ (because if we have $−n | \alpha − \beta$, then $n | −n | \alpha − \beta$). Combining these two implications, we obtain the equivalence

$(n | \alpha − \beta) \iff (−n | \alpha − \beta)$.

Now, we have the following chain of equivalences:

$$
\left( \frac{\alpha \equiv \beta}{n} \right) \\
\iff (\alpha \equiv \beta \mod n) \quad \left( \text{by the definition of the relation } \equiv_n \right) \\
\iff (n | \alpha − \beta) \quad \left( \text{by the definition of congruence} \right) \\
\iff (−n | \alpha − \beta) \quad \left( \text{by the definition of congruence} \right) \\
\iff (\alpha \equiv \beta \mod −n) \quad \left( \text{by the definition of congruence} \right) \\
\iff \left( \frac{\alpha \equiv \beta}{n} \right). \quad \left( \text{by the definition of the relation } \equiv_n \right)
$$

In other words, the two statements $\left( \frac{\alpha \equiv \beta}{n} \right)$ and $\left( \frac{\alpha \equiv \beta}{n} \right)$ 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

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

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

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

(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 $\phi$, which behaves slightly differently when being squared.

It is easy to see (from the definition of $\phi$) 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, $\alpha$ 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

$$\alpha = x_1 + x_2 \phi \quad \text{and} \quad \beta = y_1 + y_2 \phi.$$ 

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

$$\alpha - \beta = (x_1 + x_2 \phi) - (y_1 + y_2 \phi) = (x_1 - y_1) + (x_2 - y_2) \phi.$$
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

\[
\begin{align*}
\alpha &= (x_1 + x_2\phi)(y_1 + y_2\phi) = x_1y_1 + x_1y_2\phi + x_2\phi y_1 + x_2\phi y_2 \\
\beta &= (x_1 + x_2\phi)(y_1 + y_2\phi) = x_1y_1 + x_1y_2\phi + x_2\phi y_1 + x_2\phi y_2 \\
&= x_1y_1 + x_1y_2\phi + x_2\phi y_1 + x_2\phi y_2 \\
&= x_1y_1 + x_1y_2\phi + x_2y_1\phi + x_2y_2\phi \\
&= x_1y_1 + x_1y_2\phi + x_2y_1\phi + x_2y_2(\phi + 1) \\
&= (x_1y_1 + x_2y_2) + (x_1y_2 + x_2y_1 + x_2y_2)\phi.
\end{align*}
\]

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 $\phi$, which has a slightly different reason to be irrational.

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

Clearly, $\alpha$ can be written as $a + b\phi$ for at least one pair $(a, b)$ of integers (because this is what it means for $\alpha$ to belong to $\mathbb{Z}[\phi]$). Thus, it remains to prove that $\alpha$ 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. 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 $\phi = \frac{1 + \sqrt{5}}{2}$, we obtain $2\phi = 1 + \sqrt{5}$, so that $\sqrt{5} = 2\phi - 1$. Hence, if the number $\phi$ was rational, then $\sqrt{5}$ would be rational as well, which would contradict the fact that $\sqrt{5}$ is irrational. Hence, the number $\phi$ cannot be rational. In other words, $\phi$ 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, $a_2 + b_2\phi = a_1 + b_1\phi$, so that

\[
a_2 - a_1 = b_1\phi - b_2\phi = (b_1 - b_2)\phi.
\]

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, $u^2 \in \{(-2)^2, (-1)^2, 0^2, 1^2, 2^2\} = \{4, 1, 0, 1, 4\}$. 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 \( a_2 - a_1 = (b_1 - b_2) \phi = 0 \), which would lead to \( a_1 = a_2 \) and therefore \( \left( \frac{a_1}{a_2}, \frac{b_1}{b_2} \right) = (a_2, b_2) \); 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 \( \frac{a_2 - a_1}{b_1 - b_2} = \phi \). Hence, the number \( \frac{a_2 - a_1}{b_1 - b_2} \) is irrational (since \( \phi \) is irrational). But this contradicts the fact that \( \frac{a_2 - a_1}{b_1 - b_2} \) 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 \( \mathbb{Z} \) 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 \( \gamma \). From \( a \gamma = b \neq 0 \), we obtain \( a \neq 0 \).

We have \( \gamma \in \mathbb{Z}[\phi] \). In other words, \( \gamma \) 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

\[
b = a \gamma = a (x_1 + x_2 \phi) = ax_1 + ax_2 \phi.
\]

If we had \( ax_2 \neq 0 \), then we could solve this equality for \( \phi \) and obtain \( \phi = \frac{b - ax_1}{ax_2} \); this would yield that \( \phi \) is rational (since \( b, a, x_1, x_2 \) are integers), and this would contradict the fact that \( \phi \) 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, \( \gamma = x_1 + x_2 \phi = x_1 \in \mathbb{Z} \). 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 \( \phi^d, \phi^{dn}, \psi^d \) and \( \psi^{dn} \) belong to \( \mathbb{Z}[\phi] \) (since \( \phi \) and \( \psi \) 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

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

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

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

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

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

and

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

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 $\delta$. 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 $\mathbb{Z}[\sqrt{-3}]$

6.1 PROBLEM

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

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

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

(a) Prove that each 3-Gaussian integer $\alpha$ satisfies $N(\alpha) \in \mathbb{N}$ and $N(\alpha) \neq 2 \mod 3$.
(Recall that \( N(\alpha) \) is defined for every complex number \( \alpha \), and thus for every 3-Gaussian integer \( \alpha \), since 3-Gaussian integers are complex numbers.)

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

If \( \alpha \in \mathbb{Z}[\sqrt{-3}] \), then a 3-Gaussian divisor of \( \alpha \) shall mean a \( \beta \in \mathbb{Z}[\sqrt{-3}] \) such that \( \beta \mid \alpha \) in \( \mathbb{Z}[\sqrt{-3}] \).

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 \( \pi \) that is not a unit is called a 3-Gaussian prime if each 3-Gaussian divisor of \( \pi \) is either a unit or unit-equivalent to \( \pi \).

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

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

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

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

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

[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 \( \mathbb{Z}[\sqrt{-3}] \) 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 \( \alpha \) 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 \( \alpha = a + b\sqrt{-3} = \sqrt{3}i = a + b\sqrt{3}i = (a, b\sqrt{3}) \) (regarded as a complex number). Hence, the definition of the norm of a complex number yields \( N(\alpha) = a^2 + (b\sqrt{3})^2 = a^2 + 3b^2 \in \mathbb{N} \) (since \( a^2 \) and \( b^2 \) are squares of integers and therefore belong to \( \mathbb{N} \)). It remains to prove that \( N(\alpha) \neq 2 \mod 3 \).

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, \( N(\alpha) = a^2 + 3b^2 \equiv a^2 \equiv 4 \neq 2 \mod 3 \). Thus, our claim \( N(\alpha) \neq 2 \mod 3 \) 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 \( \alpha \) having norm \( N \) by a straightforward exhaustive check of all possible cases. Indeed, if \( \alpha \) is a 3-Gaussian integer having norm \( N \), then we can write \( \alpha \) in the form \( \alpha = a + b\sqrt{-3} \) for some \( a, b \in \mathbb{Z} \) (since \( \alpha \) is a 3-Gaussian integer), and then we have \( N = N(\alpha) = a^2 + 3b^2 \) (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 \( N = a^2 + 3b^2 \geq a^2 \) and \( N = a^2 + 3b^2 \geq 2 + b^2 \geq b^2 \), 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 \( \alpha \) is a unit in \( \mathbb{Z} \left[ \sqrt{-3} \right] \), then \( \alpha = 1 \) or \( \alpha = -1 \).

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

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

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

But \( \alpha \alpha^{-1} = 1 \) and thus \( N(\alpha \alpha^{-1}) = N(1) = 1^2 = 1 \), so that \( 1 = N (\alpha \alpha^{-1}) = N(\alpha) \cdot N(\alpha^{-1}) \). This leads to \( N(\alpha) \mid 1 \) (since \( N(\alpha^{-1}) \in \mathbb{N} \)). Therefore, \( N(\alpha) = 1 \) (since \( N(\alpha) \in \mathbb{N} \)). In other words, \( \alpha \) 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 \( \alpha \) is either 1 or \(-1\). In other words, \( \Box \)](\cite{source})

\[ \square \] Here is a simpler way of proving this: We know that \( \alpha \) 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 \( N(\alpha) = a^2 + 3b^2 \) (as we have already shown when solving part (a) of this exercise), so that \( a^2 + 3b^2 = N(\alpha) = 1 \). 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 \( \delta \) be a 3-Gaussian divisor of 2. We must prove that \( \delta \) 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 \( \delta \) is a 3-Gaussian divisor of 2. In other words, there exists a 3-Gaussian integer \( \gamma \) such that \( 2 = \delta \gamma \). Consider this \( \gamma \). From \( 2 = \delta \gamma \), we obtain \( N(2) = N(\delta \gamma) = N(\delta) \cdot N(\gamma) \), so that \( N(\delta) \cdot N(\gamma) = N(2) = 2^2 = 4 \).

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

- **Case 1:** We have \( N(\delta) = 1 \).
- **Case 2:** We have \( N(\delta) = 4 \).

Let us first consider Case 1. In this case, we have \( N(\delta) = 1 \). In other words, \( \delta \) has norm 1. Hence, \( \delta \) is a unit (since all 3-Gaussian integers having norm 1 are units). Thus, our claim (that \( \delta \) 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 \( N(\delta) = 4 \). Comparing \( N(\delta) \cdot N(\gamma) = 4 \) with \( N(\delta) \cdot N(\gamma) = 4 \cdot N(\gamma) \), we obtain \( 4 \cdot N(\gamma) = 4 \), so that \( N(\gamma) = 1 \). Thus, \( \gamma \) has norm 1, and therefore \( \gamma \) is a unit (since all 3-Gaussian integers having norm 1 are units). Hence, 2 is unit-equivalent to \( \delta \) (since \( 2 = \delta \gamma = \gamma \delta \)). In other words, \( \delta \) is unit-equivalent to 2 (since unit-equivalence is an equivalence relation). Thus, our claim (that \( \delta \) 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 \( \delta \) 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 \( \geq 1 \) (since the square of a nonzero integer is always \( \geq 1 \)), and thus we would have \( \frac{a^2}{\geq 0} + \frac{b^2}{\geq 1} \geq 0 + 3 \cdot 1 = 3 > 1 \), 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 \( a = a + b \cdot \sqrt{-3} = a \). Thus, \( a \) 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 $\gamma$ and $\rho$ such that $\alpha = \gamma \beta + \rho$ and $N(\rho) < N(\beta)$. Consider these $\gamma$ and $\rho$. Solving the equation $\alpha = \gamma \beta + \rho$ for $\gamma$, we obtain $\gamma = \frac{\alpha - \rho}{\beta}$ (since $\beta \neq 0$).

A straightforward computation reveals that $N(\beta) = 4$. Hence, $N(\rho) < N(\beta) = 4$. Thus, $\rho$ 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 $-\sqrt{-3}$. This gives five possible cases to check. In each of these five cases, we can compute $\gamma$ from $\gamma = \frac{\alpha - \rho}{\beta}$. We thus obtain the following table of values of $\gamma$:

<table>
<thead>
<tr>
<th>$\rho$</th>
<th>0</th>
<th>1</th>
<th>$-1$</th>
<th>$\sqrt{-3}$</th>
<th>$-\sqrt{-3}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\gamma$</td>
<td>$\frac{1}{2} - \frac{1}{2}\sqrt{-3}$</td>
<td>$\frac{1}{4} - \frac{1}{4}\sqrt{-3}$</td>
<td>$\frac{3}{4} - \frac{3}{4}\sqrt{-3}$</td>
<td>$-\frac{1}{4} - \frac{3}{4}\sqrt{-3}$</td>
<td>$\frac{5}{4} - \frac{1}{4}\sqrt{-3}$</td>
</tr>
</tbody>
</table>

(We have used the standard strategy of rationalizing denominators in order to compute these values of $\gamma$.) This table makes it clear that (in each of the five cases) $\gamma$ 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 $\gamma$ can be written in the form $\gamma = a + b\sqrt{-3}$ with some $a, b \in \mathbb{Z}$ (because $\gamma \in \mathbb{Z}[\sqrt{-3}]$). Thus, there are (at least) two different ways to write $\gamma$ in the form $\gamma = a + b\sqrt{-3}$ with some numbers $a, b \in \mathbb{Q}$. 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, $a = \Re z$ and $b = \Im z/\sqrt{3}$). This contradiction shows that our assumption was false. Hence, part (f) of the exercise is solved.

**REFERENCES**


---

*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.*